全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导

（下午科目）

工业和信息化部教育与考试中心 推荐

刘立军 宋白玉 主编 / 石鲁生 鲁建芳 史国川 副主编

第4版

清华大学出版社

VISIT…

LANZAROTE Caliente.COM

全国计算机技术与软件专业技术资格(水平)考试参考用书

网络工程师考试同步辅导
(下午科目)(第4版)

刘立军　宋白玉　主　编
石鲁生　鲁建芳　史国川　副主编

清华大学出版社
北　京

内 容 简 介

本书是按照国家人力资源和社会保障部、工业和信息化部最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材编写的考试辅导书。全书共分为6章，主要包括网络系统规划和设计、交换机配置与VLAN、路由器与网络互联、Windows应用服务器的配置、Linux应用服务器的配置、网络安全等内容，主要从考试大纲要求、考点辅导、典型例题分析和同步练习几个方面对各部分内容进行系统的阐释。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合备考网络工程师的考生使用，也可作为高等院校或培训班的教材。

封面贴有清华大学出版社防伪标签，无上述标识者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

网络工程师考试同步辅导(下午科目)/刘立军，宋白玉主编. —4版. —北京：清华大学出版社，2018
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 978-7-302-50546-4

Ⅰ. ①网…　Ⅱ. ①刘…　②宋…　Ⅲ. ①计算机网络—资格考试—自学参考资料　Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2018)第145365号

责任编辑：魏　莹　李玉萍
封面设计：常雪影
责任校对：李玉茹
责任印制：丛怀宇
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn, 010-62791865
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　**印　张：**20　**插　页：**2　**字　数：**492千字
版　　次：2005年6月第1版　2018年8月第4版　**印　次：**2018年8月第1次印刷
定　　价：59.00元

产品编号：071159-01

前　言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了二十多年，在社会上产生了很大的影响，其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求，国家人力资源和社会保障部同工业和信息化部在 2009 年对网络工程师级别考试大纲进行了重新调整，以满足社会上对各种信息技术人才的需求。本书第 1 版自 2005 年出版以来，被众多考生选用为考试参考书，多次重印，深受广大读者好评。本书第 3 版、第 2 版对第 1 版同名书进行了修订。根据网络新技术的发展，第 4 版依据最新教程进行修订，并将最新考试真题贯穿其中。为了帮助考生复习迎考，修订后本书的特色如下。

(1) 知识点全面。本书与最新网络工程师考试大纲考试科目 2——网络系统设计与管理基本一致，又兼顾网络技术发展和知识更新，对属于大纲要求的知识点但指定教材没有阐述的部分进行了必要的补充。

(2) 结构与官方教程同步。本书参考最新指定官方教程、最新考试大纲及最新题型编写章名、节名，便于考生使用《网络工程师教程(第 5 版)》进行同步复习，同时更加突出重点与难点，针对性强，减轻考生复习的工作量。

(3) 例题与习题经典。最近四年(2014—2017 年)8 次考试真题全部被分类解析到例题中，并在其中增加了根据最新考试大纲精心设计的例题，这些例题均具有典型性和代表性，而 2014 年及之前的考试真题被分类归入同步练习中，使考生能从以前的考题中更好地了解考试的难度与广度，顺利地通过考试。

(4) 重点突出。第 4 版沿袭前两版的框架，每一小节分为 4 个模块：考点辅导、典型例题分析、同步练习和同步练习参考答案。其中，考点辅导部分主要以专题的方式，重点介绍网络工程师下午考试所需的各个方面的知识；典型例题分析是本书的重点，它详尽细致地剖析了所有近四年(2014—2017 年)的真题和例题；同步练习中的每一道题都配有标准的答案，对读者所学的知识和能力可起到巩固、拓宽和提高的作用。

(5) 语言更准确，概念更清晰，能覆盖所有大纲考点，并突出重点、难点。

(6) 对书中所有例题与习题进行了精选，确保所有题目符合考纲要求。例题选取典型、有梯度、有广度，分析详尽；题目的难易度、分布率与真实考试相当；题目答案正确、解析科学。

本书可作为备考网络工程师的考生的辅导用书，也可作为高等院校相关专业或培训班的教材。

本书由刘立军、宋白玉担任主编，石鲁生、鲁建芳、史国川担任副主编，参与本书组织、编写和资料收集的还有谢瑜、周胜、鲁磊纪、杨章静、刁爱军、陈海峰、赵晗、吴敏、王华君、陶佳、徐国明、何光明等。在此对原作品作者及全体参与人员表示衷心的感谢。在本书编写的过程中，参考了许多相关的书籍和资料，从中汲取了许多营养，在此也对这些

参考文献的作者表示感谢。需要特别感谢的是来自互联网的各位不知道姓名的网友们的无私奉献，正是由于你们，才使本书的内容更完善、更详尽。

由于时间仓促和作者水平所限，书中难免存在错漏和不妥之处，敬请广大读者批评指正。联系邮箱：iteditor@126.com。

编　者

网络工程师考试(下午)考点分布导航图

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 1 章 网络系统规划和设计	1.1 网络系统的需求分析									①网络系统的需求分析。 ②网络系统的设计。 ③网络系统的构建和测试	**阅读建议** 本章对应《网络工程师教程(第 5 版)》(清华大学出版社出版，以下简称“教程”)的第 12 章“网络规划和设计”，并结合新大纲的要求在章节安排上作了适当的调整。考生可以对照教程相关内容进行同步复习	本章内容在网络规划和设计中是很重要的一部分，也是大纲中要求重点掌握的内容
	1.2 网络系统的设计	园区网的部署(20 分)	企业网的规划与部署(20 分)		工业园区网的组建(20 分)		企业网的规划设计(20 分)	企业网的设计(20 分)				
	1.3 网络系统的构建和测试			企业网的组建(20 分)					企业网的安全管理与配置(20 分)			
	1.4 网络系统的运行和维护											
	1.5 网络系统的管理和评价											
第 2 章 交换机配置与 VLAN	2.1 交换机的基本配置		交换机的配置(15 分)	交换机的配置(15 分)	交换机的配置(35 分)					①交换机的配置，包括命令行接口配置、Web 方式访问交换机。 ②VLAN 配置。 ③多层交换机功能和机制	**阅读建议** 本章对应教程第 10 章“组网技术”中的 10.1 节“交换机和路由器”和 10.2 节“交换机的配置”。考生可以对照教程相关内容进行同步复习	本章考点分值约占总考分的 15%。通常考查交换机的基本配置以及 VLAN 的实施，包括 STP 和 VTP 等。高频考点为: ◆VLAN。 ◆STP。 ◆VTP
	2.2 VLAN 的配置											

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 3 章 路由器与网络互联	3.1 IP 地址与划分									①路由器的配置，包括命令行接口配置、Web 方式访问路由器、VOIP 配置、路由协议的配置、广域联网、DTP、STP、RSTP。 ②远程访问服务器，包括功能和机制。 ③网络接入与服务，包括 HFC 、ADSL 、FTTx＋LAN 、WLAN 、移动通信、服务供应商、因特网广播、电子商务、电子政务、主机服务提供者、数据中心。 ④IP 路由器功能和控制	**阅读建议** 本章对应教程第 10 章“组网技术”中的 10.1 节“交换机和路由器”、10.3 节“路由器的配置”、104 节“配置路由协议”和 10.5 节“配置广域网接入”。考生可以对照教程相关内容进行同步复习	本章考点分值约占总考分的 20%。通常考查 IP 地址的规划、路由器的基本配置以及路由协议的相关配置，还有常见的网络接入技术。高频考点为： ◆路由器的基本配置。 ◆OSPF 路由配置。 ◆RIP 路由配置。 ◆ACL 配置。 ◆WLAN
	3.2 路由器的配置与网络互联	路由器的配置(15 分)	路由器的配置(20 分)			路由器的配置(20 分)	路由器的配置(15 分)	路由器的配置(15 分)	路由器的配置(15 分)			
	3.3 网络接入方式											
第 4 章 Windows 应用服务器的配置	4.1 IIS 服务器的配置	IIS 服务器的配置(20 分)	IIS 服务器的配置(20 分)		Windows Server 2003 服务器 Web、FTP 和邮件服务配置(20 分)				Windows 下路由和远程服务的配置(20 分)	①IP 地址，包括 IPv4、IPv6、动态分配和静态分配、DHCP 服务器的原理和配置(Windows)。 ②网络系统管理，包括网络管理命令、Windows 系统、Windows 活动目录、Windows 终端服务与远程管理。 ③DNS，包括 URL、域名解析、DNS 服务器的配置(Windows)。 ④电子邮件服务器的配置(Windows)。 ⑤WWW，包括虚拟主机、WWW 服务。 ⑥服务器配置(Windows)、WWW 服务器的安全配置。 ⑦代理服务器的配置(Windows)。 ⑧FTP 服务器，包括 FTP 服务器的访问、FTP 服务器的配置(Windows)	**阅读建议** 本章对应教程第 9 章“网络操作系统与应用服务器配置”中的 9.1 节“网络操作系统”、9.2 节“网络操作系统的基本配置”、9.3 节“Windows Server 2008 R2 IIS 服务器的配置”、9.5 节“DNS 服务器的配置”、9.6 节“DHCP 服务器的配置”和 9.7 节“电子邮件服务器的配置”。考生可以对照教程相关内容进行同步复习	本章考点分值约占总考分的 18%。通常考查 Windows 网络服务的基本功能以及在 Windows 平台下相关服务器的配置，主要包括 IIS 服务器的配置、DNS 服务器的配置、DHCP 服务器的配置和代理服务器的配置。高频考点为： ◆DNS 服务器的配置。 ◆DHCP 服务器的配置。 ◆IIS 服务器的配置
	4.2 DNS 服务器的配置					Windows 下 DNS 的配置(15 分)	Windows 下 Web、DNS 的配置(20 分)	Windows 下 DNS 的配置(20 分)				
	4.3 DHCP 服务器的配置			Windows 下 DHCP 服务器的配置(20 分)		Windows 下 DHCP 服务器的配置(15 分)						
	4.4 代理服务器的配置											

续表

章	节	历年真题分布								大纲要求	阅读链接	命题预测
		2014.05	2014.11	2015.05	2015.11	2016.05	2016.11	2017.05	2017.11			
第 5 章 Linux 应用服务器的配置	5.1 Apache 服务器的配置									①DHCP 服务器的原理和配置(Linux)。 ②DNS，包括 URL、域名解析、DNS 服务器的配置(Linux)。 ③电子邮件服务器的配置(Linux)。 ④WWW，包括虚拟主机、WWW 服务器配置(Linux)、WWW 服务器的安全配置。 ⑤FTP 服务器，包括 FTP 服务器的访问、FTP 服务器的配置(Linux)	**阅读建议** 本章对应教程第 9 章“网络操作系统与应用服务器配置”中的 9.1 节“网络操作系统”、9.2 节“网络操作系统的基本配置”、9.4 节 Linux Apache、9.5 节“DNS 服务器的配置”、9.6 节“DHCP 服务器的配置”和 9.7 节“Samba 服务器的配置”。考生可以对照教程相关内容进行同步复习	本章考点分值约占总考分的 17%。通常考查 Linux 网络服务的基本功能以及相关服务器的配置，主要包括 Apache 服务器的配置、DNS 服务器的配置、DHCP 服务器的配置和 Samba 服务器的配置。高频考点为： ◆DNS 服务器的配置。 ◆DHCP 服务器的配置。 ◆Apache 服务器的配置
	5.2 DNS 服务器的配置	Linux 下 DNS 的配置(15 分)										
	5.3 DHCP 服务器的配置	Linux 下 DHCP 的配置(15 分)		Linux 下 DHCP 的配置(20 分)								
	5.4 Samba 服务器的配置											
第 6 章 网络安全	6.1 防火墙配置					防火墙的配置(20 分)	防火墙的配置(20 分)	防火墙的配置(20 分)	防火墙的配置(20 分)	① 访问控制与防火墙，包括 ACL 命令、过滤规则、防火墙配置。 ② 数字证书。 ③ VPN 配置。 ④ PGP。 ⑤ 病毒防护	**阅读建议** 本章对应教程第 8 章“网络安全”，并根据下午考试科目的特点，在章节安排上作了相应调整。考生可以对照教程相关内容进行同步复习	本章考点分值约占总考分的 30%。通常考查防火墙的知识和访问控制策略，包括 ACL 命令、过滤规则、Cisco PIX 防火墙的配置和 VPN 的实现与配置，还有一些病毒防护的知识。高频考点为： ◆ACL 命令。 ◆VPN 的实现与配置。 ◆Cisco PIX 防火墙的配置
	6.2 VPN 配置											
	6.3 病毒防护											

目　　录

第 1 章　网络系统规划和设计 1

1.1　网络系统的需求分析 2

1.1.1　考点辅导 2

1.1.2　典型例题分析 7

1.1.3　同步练习 11

1.1.4　同步练习参考答案 11

1.2　网络系统的设计 12

1.2.1　考点辅导 12

1.2.2　典型例题分析 21

1.2.3　同步练习 26

1.2.4　同步练习参考答案 28

1.3　网络系统的构建和测试 29

1.3.1　考点辅导 29

1.3.2　典型例题分析 43

1.3.3　同步练习 43

1.3.4　同步练习参考答案 43

1.4　网络系统的运行和维护 44

1.4.1　考点辅导 44

1.4.2　典型例题分析 55

1.4.3　同步练习 55

1.4.4　同步练习参考答案 56

1.5　网络系统的管理和评价 57

1.5.1　考点辅导 57

1.5.2　典型例题分析 92

1.5.3　同步练习 96

1.5.4　同步练习参考答案 97

1.6　本章小结 97

第 2 章　交换机配置与 VLAN 98

2.1　交换机的基本配置 98

2.1.1　考点辅导 98

2.1.2　典型例题分析 101

2.1.3　同步练习 111

2.1.4　同步练习参考答案 113

2.2　VLAN 的配置 113

2.2.1　考点辅导 113

2.2.2　典型例题分析 117

2.2.3　同步练习 120

2.2.4　同步练习参考答案 123

2.3　本章小结 124

第 3 章　路由器与网络互联 125

3.1　IP 地址与划分 125

3.1.1　考点辅导 125

3.1.2　典型例题分析 130

3.1.3　同步练习 132

3.1.4　同步练习参考答案 132

3.2　路由器的配置与网络互联 133

3.2.1　考点辅导 133

3.2.2　典型例题分析 145

3.2.3　同步练习 152

3.2.4　同步练习参考答案 155

3.3　网络接入方式 156

3.3.1　考点辅导 156

3.3.2　典型例题分析 158

3.3.3　同步练习 160

3.3.4　同步练习参考答案 161

3.4　本章小结 161

第 4 章　Windows 应用服务器的配置 162

4.1　IIS 服务器的配置 162

4.1.1　考点辅导 162

4.1.2　典型例题分析 167

4.1.3　同步练习 177

4.1.4　同步练习参考答案 180

4.2　DNS 服务器的配置 182

4.2.1　考点辅导 182

4.2.2　典型例题分析 189

4.2.3　同步练习 191

4.2.4　同步练习参考答案 193

4.3 DHCP 服务器的配置........................194
4.3.1 考点辅导........................194
4.3.2 典型例题分析........................202
4.3.3 同步练习........................211
4.3.4 同步练习参考答案........................212
4.4 代理服务器的配置........................213
4.4.1 考点辅导........................213
4.4.2 典型例题分析........................219
4.4.3 同步练习........................221
4.4.4 同步练习参考答案........................223
4.5 本章小结........................224

第 5 章 Linux 应用服务器的配置........................225

5.1 Apache 服务器的配置........................225
5.1.1 考点辅导........................225
5.1.2 典型例题分析........................232
5.1.3 同步练习........................240
5.1.4 同步练习参考答案........................241
5.2 DNS 服务器的配置........................242
5.2.1 考点辅导........................242
5.2.2 典型例题分析........................248
5.2.3 同步练习........................252
5.2.4 同步练习参考答案........................254
5.3 DHCP 服务器的配置........................254
5.3.1 考点辅导........................254
5.3.2 典型例题分析........................256
5.3.3 同步练习........................257
5.3.4 同步练习参考答案........................259
5.4 Samba 服务器的配置........................259
5.4.1 考点辅导........................259
5.4.2 典型例题分析........................262
5.4.3 同步练习........................265
5.4.4 同步练习参考答案........................267
5.5 本章小结........................268

第 6 章 网络安全........................269

6.1 防火墙配置........................269
6.1.1 考点辅导........................269
6.1.2 典型例题分析........................274
6.1.3 同步练习........................279
6.1.4 同步练习参考答案........................280
6.2 VPN 配置........................282
6.2.1 考点辅导........................282
6.2.2 典型例题分析........................292
6.2.3 同步练习........................295
6.2.4 同步练习参考答案........................300
6.3 病毒防护........................303
6.3.1 考点辅导........................303
6.3.2 典型例题分析........................306
6.3.3 同步练习........................309
6.3.4 同步练习参考答案........................310
6.4 本章小结........................310

参考文献........................311

第 1 章　网络系统规划和设计

大纲要求：

- 应用需求分析，包括应用需求的调研、网络应用的分析。
- 现有网络系统分析，包括现有网络系统结构调研、现有网络体系结构分析。
- 需求分析，包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求、管理需求。
- 技术和产品的调研及评估，包括收集信息、采用的技术和产品的比较研究、采用的技术和设备的比较要点。
- 网络系统的设计，包括确定协议、确定拓扑结构、确定连接(链路的通信性能)、确定节点(节点的处理能力)、确定网络的性能、确定可靠性措施、确定安全性措施、网络设备的选择、制定选择标准、通信子网的设计、资源子网的设计。
- 新网络业务运营计划。
- 设计评审。
- 安装工作。
- 测试和评估。
- 转换到新网络的工作计划。
- 用户措施，包括用户管理、用户培训、用户协商。
- 制订维护和升级的策略和计划，包括确定策略、设备的编址、审查的时间、升级的时间。
- 维护和升级的实施，包括外部合同要点、内部执行要点。
- 备份与数据恢复，包括数据的存储与处置、备份、数据恢复。
- 网络系统的配置管理，包括设备管理、软件管理、网络配置图。
- 网络系统的监视，包括网络管理协议(SNMP、MIB-2、RMON)、利用工具监视网络性能、利用工具监视网络故障、利用工具监视网络安全(入侵检测系统)、性能监视的检查点、安全监视的检查点。
- 故障恢复分析，包括故障分析要点(LAN 监控程序)、排除故障要点、故障报告的撰写要点。
- 系统性能分析，包括性能要点。
- 危害安全的对策，包括危害安全的情况分析、入侵检测要点、对付计算机病毒的要点。
- 系统评价，包括系统能力的限制、潜在的问题分析、系统评价要点。
- 改进系统的建议，包括系统生命周期、系统经济效益、系统的可扩充性。

1.1 网络系统的需求分析

1.1.1 考点辅导

1.1.1.1 应用需求分析

1. *应用需求的调研*

需求分析是构建网络的第一个阶段，通过需求分析，可以帮助网络设计者更好地理解网络功能，更好地评价现有网络，更客观地做出决策；有助于为网络设计者提供更加完善的交互功能和移植功能，使其更合理地使用用户资源等。

应用需求的调研内容包括应用系统性能、信息产生和接收点、数据量和频度、数据类型和数据流向等。

1) 应用系统性能

用户系统中的应用有许多类型，其中一些应用在整个系统中占有相当重要的地位。应用系统的性能往往是用户最为关注的，常见的性能指标包括可靠性/可用率、响应时间、安全性、可实现性和实时性等。

2) 信息产生和接收点

网络上的信息流都有其产生和接收的位置，产生信息的称为源，接收信息的则称为宿(即目的)。在进行需求分析时，分清信息的源和宿是非常必要的。

3) 数据量和频度

网络中的通信类型包括数据、视频信号和音频信号等，不同类型的流量使用不同的量度。数据的流量一般用平均或高峰时每秒传送的位数(比特每秒，简写为 bps)来表示；视频信号的流量用电视通道数来表示，每个通道占 6 MHz 带宽；音频信号的流量则用欧拉数来表示。

频度是指数据在单位时间内传送的次数，不同类型的数据，传送的频度不同。

流量估计应该先分析用户的网络应用，分别估计每种应用产生的分流量，然后再把各种分流量乘以频度，累计得出系统的总流量。

准确的流量估计可以避免网络系统因带宽过窄而形成瓶颈，导致网络吞吐量和性能的下降，因此，对网络通信业务量的估计必须留有足够的余量。

4) 数据类型和数据流向

网络服务一般分为 3 种：共享数据服务、综合语音服务和多媒体应用服务。其中共享数据服务是最常见的业务，综合语音服务主要是电话类业务，而多媒体应用服务则包括语音、图形、图像等多种服务。不同的服务有不同的数据类型。

数据流向是指数据流传输的方向，在客户机/服务器工作模式中，数据的流向既可以是客户机到服务器的，也可以是服务器到客户机的。

因此，网络设计人员必须根据用户具体的应用情况，详细分析网络承载的数据类型和数据流向，合理地分配网络容量。

2. 网络应用的分析

网络的主要功能是通过数据传输实现数据共享，目前应用在科研、教育、金融证券、企业管理、制造、办公自动化、电子商务、家庭娱乐等许多领域。

网络应用按照响应时间可以分为两种：实时应用和非实时应用。不同的应用有着不同的网络响应性能需求，对网络延迟和带宽有不同的影响。

实时应用要求将节点机产生的数据立即传送出去，一般不需要用户干预。实时应用要求信息传输的速率稳定，具有可预测性。令牌传递网络(令牌环网或 FDDI)和面向连接的服务(如 ATM)可以为这些应用提供支持，但在网络分析与设计中通常不考虑实时应用。

通常所说的应用指的是非实时应用，此类应用对网络带宽和数据传输能力的要求比较高，当暂时争用不到网络介质时，只要介质可以承受任何突发性的数据收发任务，非实时应用就不会出现问题。所以，这种应用适合于类似以太网的共享介质网络。

另外，按照应用是否共享，又可以把应用分为独立应用和共享应用两种类型。

不同的应用对网络功能和性能方面的需求不同，网络设计人员应对网络应用需求加以分析，以便确定网络的应用目标及其他相关指标。

1.1.1.2　现有网络系统分析

1. 现有网络系统结构调研

如果需要在已有网络上构建新系统，那么就应该全面了解现有网络情况，尽可能考虑旧系统的利用，这样既可以保护用户原有投资，又能让用户在使用新系统时有一个平滑的过渡，从而大大节省培训的时间和费用。

网络系统的建设一般需要分成几个阶段来实施，每个阶段都是在前期网络的基础之上进行的，不可能完全抛弃现有网络。因此，必须对现有网络进行仔细调研，以考查在原有网络中哪些部分是可以利用的，哪些部分是需要升级的，哪些部分是无用而必须舍弃的。重点考查的内容有以下几个方面。

1)　服务器的数量和位置

服务器是网络中提供专门服务的设备，是网络中的稀缺资源，新网络应该尽量将它们包括进去。在建设新网络之前，需要了解清楚服务器的台数、位置、型号、使用的软件、提供的服务类型以及其他各项性能指标。

2)　客户机的数量和位置

客户机是用户使用网络服务的窗口，有的客户机只供单个用户使用，而有的则供多人使用(如图书馆的查询机)；另外，在客户机上运行的应用系统有差别，对网络服务的需求也不一样。网络中包含的客户机的数量及承担的任务决定了网络的负载，因而有关客户机的信息对网络系统的设计也非常重要，新建网络时必须仔细考虑它们。

3)　使用情况

网络的使用情况包括客户机的数量、访问类型、每天的用户数、每次使用的时间、每次数据传输的数据量、网络拥塞的时间段等，这些数据都可以通过查询网络管理系统的日志文件获得。如果没有完整的日志数据，也可以通过与用户交谈获得有用信息。这些数据虽然不需要十分准确，但其准确性将影响今后网络的设计方案。

4) 采用的协议

协议是网络通信的基础，原有网络可能包含有多种协议，协议间存在着一定的差异。这就需要进行详细的调查，以便新建网络时能够很好地照顾到多种协议间的差异，以方便不同协议数据之间的转换。

5) 通信模式

通信模式就是用户接入网络的方式。网络设计要兼顾各种通信模式。

2. 现有网络体系结构分析

网络体系结构是定义和描述一组用于计算机及其通信设备之间互联的标准和规范的集合，遵循这组规范就可以实现计算机设备之间的通信。目前有两大主流体系结构标准：一个是国际标准 OSI(开放系统互联)参考模型，另一个是工业标准 TCP/IP 模型。

OSI 参考模型通过分层和抽象，将网络划分为七个功能各异的层次，同一端系统中的低层为高层提供服务，不同端系统中的对等层之间进行通信并交换协议数据单元。它是一个开放系统模型，概念清晰，但偏重于理论研究，复杂而不实用，目前实现的范例还较少。

TCP/IP 简化了 OSI 参考模型的分层结构，层次明显减少，实现简单，功能强大，目前为大多数厂商支持，已成为网络通信协议事实上的标准，并已得到普遍的推广。其他还有 IBM 的系统网络体系结构(SNA)和 DEC 的数字网络体系结构(DNA)等。

通过对现有网络体系结构进行分析，可以为建设新网络提供参考依据。同时在设计新网络时也应该照顾到原有网络的体系结构，尽量发挥其优势，而不应该完全抛弃。

1.1.1.3 需求定义

网络系统的需求包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求以及管理需求等，下面逐一介绍。

1. 功能需求

功能需求即网络在用户单位业务中应该提供的功能，可以通过了解用户单位所从事的行业、该单位在行业内的地位以及和其他单位的关系等来确定其功能需求。另外，还可以通过了解项目背景来明确用户单位建网的目的，从而有助于描述详细的功能需求。

2. 通信需求

在网络中，网络通信是个人通信模式和流量的组合。通信模式以发生在节点(客户机)之间的通信方式为基础。通常有以下几种通信方式。

- ◆ 对等通信方式。
- ◆ 客户机/服务器通信方式。
- ◆ 服务器/客户机通信方式。

独立节点之间可以在一种或多种方式下通信，如何选择通信方式取决于网络的资源、节点和应用程序的性能。例如，在对等通信方式下，各工作站之间可共享资源；在客户机/服务器通信方式下，可以访问中央文件服务器上的核心数据库。

1) 对等通信方式

对等通信方式是在一种结构和功能相似的节点之间的通信，通信节点具有相似的应用和通信能力。在该种网络中，每个节点与网络中的其他节点相连接，没有明显的源通信模

式和目的通信模式。

2)　客户机/服务器通信方式

客户机/服务器通信方式是网络中的客户机和服务器之间的通信。客户机可以是任何类型的节点，这些节点可以访问一些共享的资源。服务器在大小和功能上有所不同，既可以是基于 PC 的服务器，也可以是中型计算机和大型计算机。

3)　服务器/客户机通信方式

数据库服务器应用程序使数据从服务器流向客户机。通常情况下，客户机请求比服务器响应所传送的通信量要少。例如，在典型的 Web 方案中，服务器根据客户机浏览器的请求向客户机发送大量的 Web 页面，这就是所说的服务器/客户机分布。

4)　相关指标

为了确定用户的通信需求，需要了解用户单位的建筑物布局、入网站点的分布情况，并记录下述信息。

- 网络中心(或计算中心)及各级设备间的位置。
- 用户数量及其位置。
- 任何两个用户之间的最大距离。
- 用户群组织(即在同一楼里或同一楼层里的用户，尤其注意那些地理上分散，却属于同一部门的用户)。
- 特殊的需求或限制(例如，网络覆盖的地理范围内是否有道路、山丘；建筑物之间是否有阻挡物；电缆等介质布线是否有禁区；是否存在可以利用的介质系统等)。

3. 性能需求

在需求分析中要分析网络的多种性能特性，包括响应时间、延迟、等待时间、利用率、带宽、容量、吞吐量、可用性、可靠性、可恢复性、冗余度、适应性、可伸缩性、效率和费用等。有些需求用户不是很关心，但对于设计者却是必须考虑的。随着计算机网络数量的增长、规模的扩大，如何提高网络性能成为十分重要的问题。与衡量单机系统的性能不同，网络性能是衡量多台计算机系统的性能。了解网络用户的需要，设定恰当的性能目标，合理选择网络结构和组成，便能得到满足用户需求且性能比较好的网络。

网络用户关心的网络性能是能否获得最快的响应，网络管理员关心的网络性能是能否获得最高的资源利用率，两者需要很好地平衡。这种平衡包括两个方面：一方面是性能和价格的折中，另一方面是吞吐量和响应时间的平衡。

4. 可靠性需求

可靠性需求就是用户需要什么样的可靠性。一个系统的可靠性定义为在指定的条件和时间内，系统能够实现指定功能的概率。而整个系统的可靠性又取决于组成系统的各个部件的可靠性。

可靠性指标一般包括平均无故障时间(MTBF)和平均修复时间(MTTR)、可用性和故障率等。

5. 安全需求

1)　安全需求概述

网络安全性包括对物理产品的布局和对过程的操作，合理的物理产品布局与安全设置

可以保护网络和系统的完整性、可行性及可靠性。现代的网络安全性是把基本的网络安全性概念运用在分布式网络环境中。网络安全性的目的是对资源的保护，目前还没有彻底的解决方法。

安全设计包括安全服务和实施两方面。原则上讲，每一个网络系统都具有独立和通用的安全协议，而基于安全服务的安全信息则是存放在管理信息库(MIB)中的，只有授权人员或系统才可访问、修改或删除这些机密信息。通过对网络易损点的识别，可使这些易损点得到保护和监控，要确保安全，应采取一种分层管理策略。

安全性策略的 3 个属性定义为保密性、完整性和可信性。信息损失通常由以下原因引起：更改、破坏和泄露。对网络安全构成威胁的形式有很多，而且它们经常导致网络失常和重要信息的毁坏。

采取何种安全措施需要视用户需要而定，不同单位或一个单位的不同部门要求的安全等级往往是有差异的，并不是安全等级越高越好，较高的安全等级意味着额外的系统开销和高昂的费用。

2) 安全性标准

网络系统是否达到一定的安全性主要依照相关的安全性标准来判断，最早的信息系统安全性标准由美国国防部颁布的黄皮书(TC-SEC-NCSC，可信计算机系统)规定。该手册将 IT 系统划分为 A(A1)、B(B1、B2、B3)、C(C1、C2)、D(D1)4 类，共 7 个安全等级。

(1) D 类安全等级。D 类安全等级只包括 D1 一个级别，D1 的安全等级最低，它只为文件和用户提供安全保护。D1 系统最常见的形式是本地操作系统，或者是一个完全没有保护的网络。

(2) C 类安全等级。C 类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。

(3) B 类安全等级。B 类安全等级可划分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能，这就意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

(4) A 类安全等级。A 类系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是：系统的设计者必须按照一个正式的设计规范来分析系统。对系统进行分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

欧洲等价的分类手册是 ITSEC(信息技术安全评估标准)。与美国的黄皮书类似，ITSEC 标准目录将 IT 系统划分为 7 个安全等级(E0～E6)，这些等级与黄皮书中的各个等级大致对应。

6. 维护和运行需求

维护和运行是网络系统投入正常运行后的日常管理工作，这项工作主要由网络管理人员承担。网络管理人员通过网络管理系统可以完成系统的配置、监控和统计等事务的处理，有时还要对网络设备进行检修。网络设计人员需要根据用户需求，提供必要的网络管理工具和策略，以方便网络管理人员对整个网络进行管理和维护，提高网络的运行效率，保证

网络的可靠性。

7. 管理需求

从用户的角度来讲，一个网络管理系统应该满足以下要求。

- 同时支持网络监视和控制两方面的能力。
- 能够管理所有的网络协议。
- 尽可能大的管理范围。
- 尽可能小的系统开销。
- 可以管理不同厂家的联网设备。
- 容纳不同的网络管理系统。
- 网络管理的标准化。

在 OSI 网络管理框架模型中，基本的网络管理功能被分为 5 个功能域：配置管理(Configuration Management)、性能管理(Performance Management)、故障管理(Fault Management)、安全管理(Security Management)和计费管理(Accounting Management)。

网络管理的标准化产品包括 ISO 的 CMIS/CMIP(Common Management Information Service/Common Management Information Protocol)、Internet 体系结构委员会(Internet Architecture Board，IAB)的 SNMP 和管理信息库(MIB)，这些内容将在第 5 章详细介绍。

1.1.2　典型例题分析

例 1　【说明】(2017 年上半年下午试题一)

某企业网络拓扑如图 1-1 所示，中国电信和中国移动双链路接入，采用硬件设备实现链路负载均衡：主磁盘阵列的数据通过备份服务器到备份磁盘阵列。请结合下图，回答相关问题。

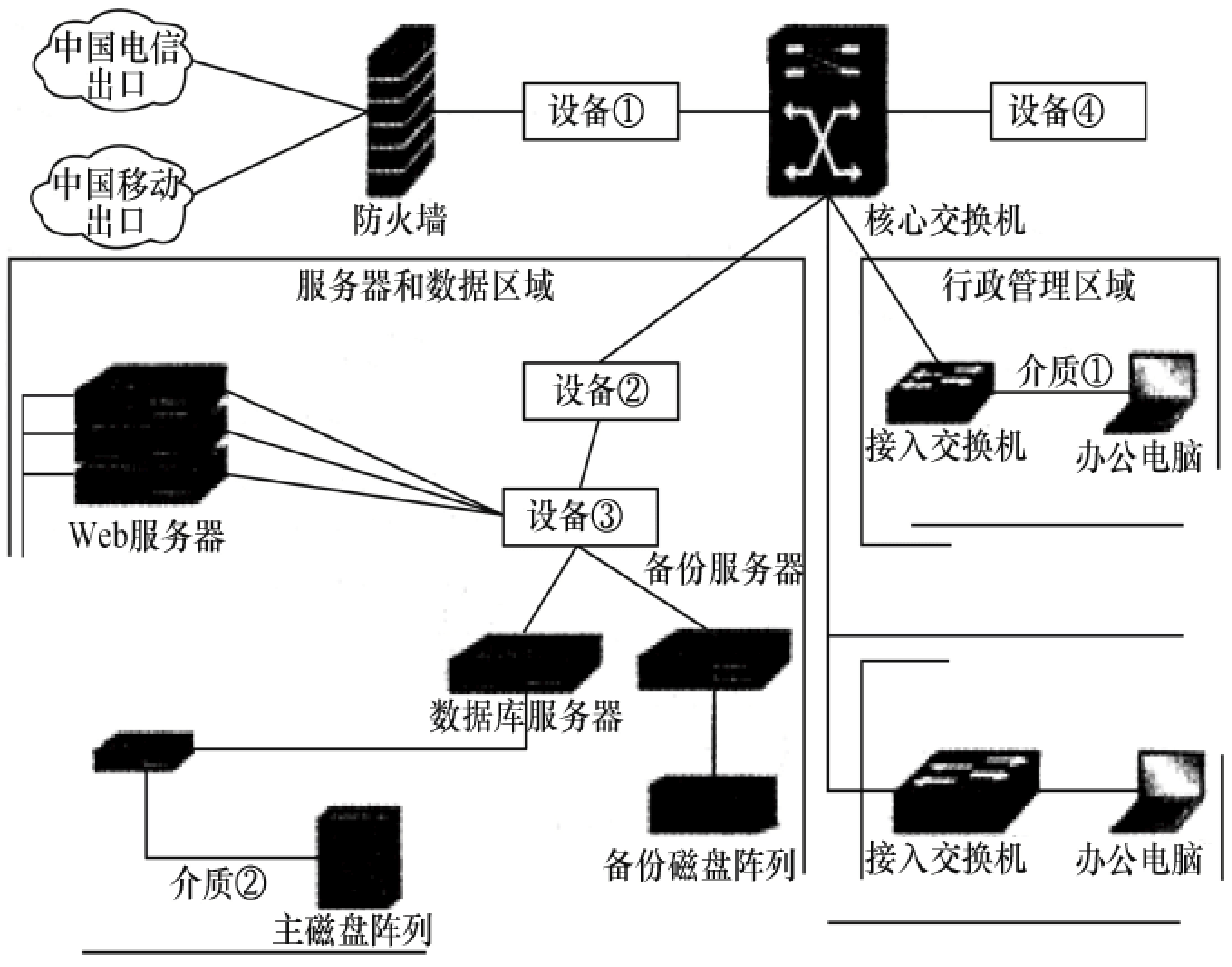


图 1-1　某企业网络拓扑

【问题 1】(共 6 分)

图 1-1 中，设备①处部署__(1)__，设备②处部署__(2)__，设备③处部署__(3)__。(1)～

(3)备选答案(每个选项限选一次):

A. 入侵防御系统(IPS)　　B. 交换机　　C. 负载均衡

【问题 2】(共 4 分)

图 1-1 中，介质①处应采用__(4)__，介质②处应采用__(5)__。

(4)～(5)备选答案(每个选项限选一次):

A. 双绞线　　B. 同轴电缆　　C. 光纤

【问题 3】(共 4 分)

图 1-1 中，为提升员工的互联网访问速度，通过电信出口访问电信网络，移动出口访问移动网络，则需要配置基于__(6)__地址的策略路由；运行一段时间后，网络管理员发现电信出口的用户超过 90%，网络访问速度缓慢，为实现负载均衡，网络管理员配置基于__(7)__地址的策略路由，服务器和数据区域访问互联网使用电信出口，行政管理区域员工访问互联网使用移动出口，生产业务区域员工使用电信出口。

【问题 4】(共 6 分)

1.图 1-1 中，设备④处应为__(8)__，该设备可对指定计算机系统进行安全脆弱性扫描和检测，发现其安全漏洞，客观评估网络风险等级。

2.图 1-1 中，__(9)__设备可对恶意网络行为进行安全检测和分析。

3.图 1-1 中，__(10)__设备可实现内部网络和外部网络之间的边界防护，依据访问规则，允许或者限制数据传输。

答案:

【问题 1】(1) C　(2) A　(3) B

【问题 2】(4) A　(5) C

【问题 3】(6) 目的　(7) 源

【问题 4】(8) 漏洞扫描设备　(9) IPS　(10) 防火墙

解析:

【问题 1】综合分析可知设备 3 是交换机，那么设备 2 为 IPS，设备 1 为负载均衡。

【问题 2】介质 1 连接接入交换机和用户，故为双绞线。介质 2 连接 FC 交换机和磁盘阵列，应为光纤。

【问题 3】访问电信网络通过电信出口，移动网络通过移动出口，这是通过访问目的来区分的，故是基于目的地址的策略路由。而后根据访问人群的划分更改为基于源地址的策略路由。

【问题 4】漏洞扫描通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检查，发现可利用的漏洞的一种安全性检测行为。在图 1-1 中 IPS 设备对恶意网络行为进行分析。防火墙设备则为内外网之间的安全保护屏障。

例 2　【说明】(2016 年下半年下午试题二)

图 1-2 是某互联网企业网络拓扑，该网络采用二层结构，网络安全设备有防火墙、入侵检测系统，楼层接入交换机 32 台，全网划分 17 个 VLAN，对外提供 Web 和邮件服务。数据库服务器和邮件服务器均安装 CentOS 操作系统(Linux 平台)，Web 服务器安装 Windows 2008 操作系统。

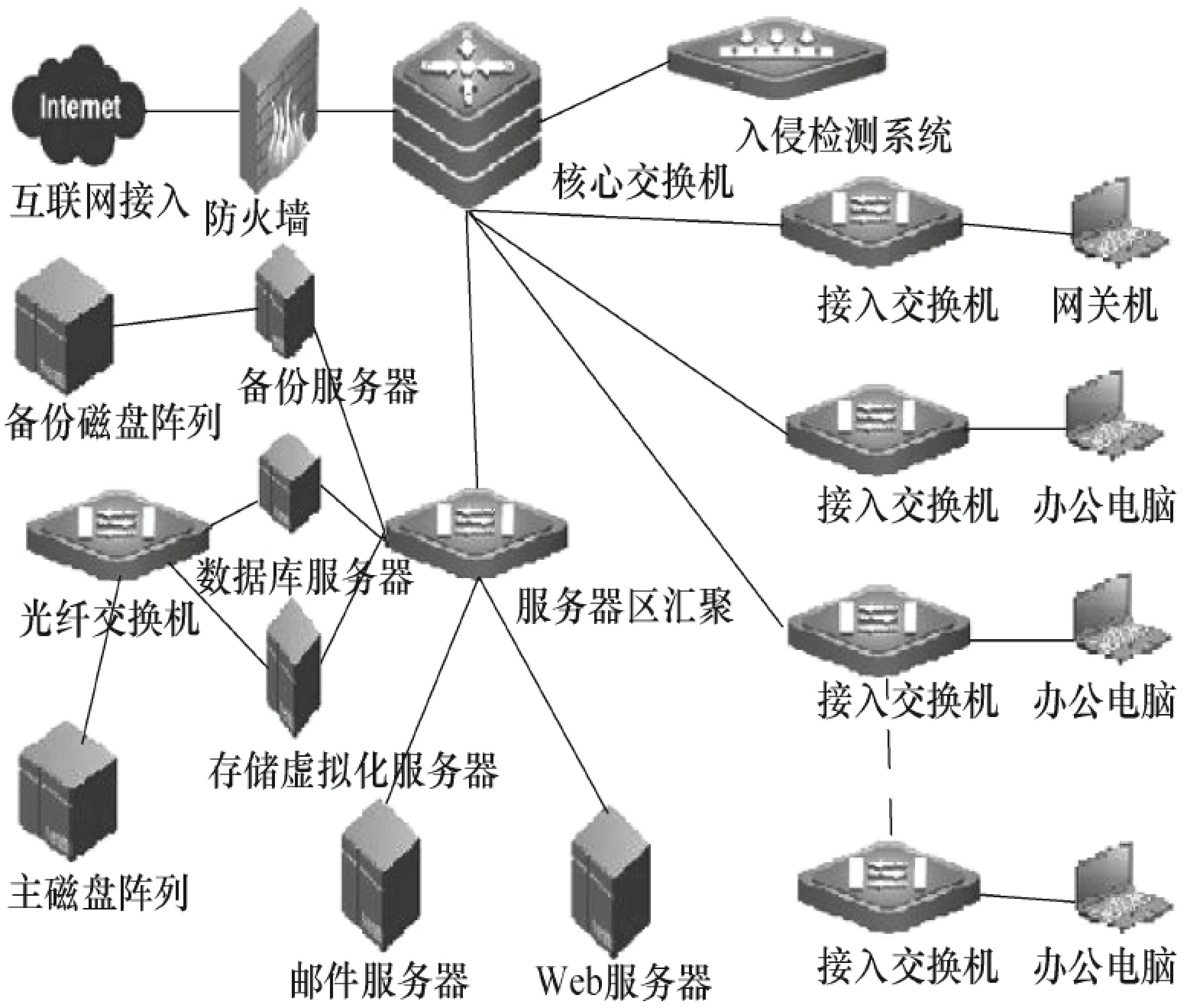


图 1-2　某互联网企业网络拓扑

【问题 1】(6 分)

SAN 常见方式有 FC-SAN 和 IP-SAN，在图 1-2 中，数据库服务器和存储设备连接方式为 __(1)__，邮件服务器和存储设备连接方式为 __(2)__。虚拟化存储常用文件系统格式有 CIFS、NFS，为邮件服务器分配存储空间时应采用的文件系统格式是 __(3)__，为 Web 服务器分配存储空间时应采用的文件系统格式是 __(4)__。

【问题 2】(3 分)

该企业采用 RAID5 方式进行数据冗余备份，请从存储效率和存储速率两个方面比较 RAID1 和 RAID5 两种存储方式，并简要说明采用 RAID5 存储方式的原因。

【问题 3】 (8 分)

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断：

1. 通过网管机，利用 __(5)__ 登录到邮件服务器，发现邮件服务正常，但是连接时断时续。

2. 使用 __(6)__ 命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区汇聚交换机 SI，发现连接邮件服务器的端口数据流量异常，收发包量很大。

3. 根据以上情况，邮件服务器的可能故障为 __(7)__，应采用 __(8)__ 的办法处理上述故障。

(5)～(8)备选答案：

(5) A. ping　　B. ssh　　C. tracert　　D. mstsc

(6) A. ping　　B. telnet　　C. tracet　　D. netstat

(7) A. 磁盘故障　　B. 感染病毒　　C. 网卡故障　　D. 负荷过大

(8) A. 更换磁盘　　B. 安装防病毒软件，并查杀病毒

C. 更换网卡　　D. 提升服务器处理能力

【问题 4】 (3 分)

上述企业网络拓扑存在的网络安全隐患有：__(9)__、__(10)__、__(11)__。

(9)～(11)备选答案：

A. 缺少针对来自局域网内部的安全防护措施

B. 缺少应用负载均衡

C. 缺少流量控制措施

D. 缺少防病毒措施

E. 缺少 Web 安全防护措施

F. 核心交换机到服务器区汇聚交换缺少链路冗余措施

G. VLAN 划分太多

答案：

【问题 1】(1) FC-SAN (2) IP-SAN (3) NFS (4) CIFS

【问题 2】

(1) 存储效率上，RAID5 的存储利用率为$(n-1)/n$，RAID1 的存储利用率为 50%，RAID5 的存储效率高。

(2) 存储速率上，RAID5 的速率快于 RAID1。

原因：RAID5 具有数据安全，读写速度快，空间利用率高、成本低的特点。

【问题 3】(5) B (6) A (7) B (8) B

【问题 4】(9) A (10) D (11) E

解析：

【问题 1】

1. SAN 主要包含 FC-SAN 和 IP-SAN 两种。

1) 存储区域网络(Storage Area Network，SAN)：存储设备组成单独的网络，大多利用光纤连接，采用光纤通道协议(Fiber Channel，FC)。服务器和存储设备间可以任意连接，I/O 请求也是直接发送到存储设备。光纤通道协议实际上解决了底层的传输协议，高层的协议仍然采用 SCSI 协议，所以光纤通道协议实际上可以看成是 SCSI over FC。

2) IP-SAN：由于 FC-SAN 的高成本使得很多中小规模存储网络不能接受，一些人开始考虑构建基于以太网技术的存储网络。但是在 SAN 中，传输的指令是 SCSI 的读写指令，不是 IP 数据包。iSCSI(互联网小型计算机系统接口)是一种在 TCP/IP 上进行数据块传输的标准。它是由 Cisco 和 IBM 两家公司发起的，并且得到了各大存储厂商的大力支持。iSCSI 可以实现在 IP 网络上运行 SCSI 协议，使其能够在诸如高速千兆以太网上进行快速的数据存取备份操作。为了与之前基于光纤技术的 FC-SAN 区分开来，这种技术被称为 IP-SAN。iSCSI 继承了两大最传统技术：SCSI 和 TCP/IP 协议。这为 iSCSI 的发展奠定了坚实的基础。

2. CIFS 和 NFS。

1) CIFS(Common Internet File System)是由 Microsoft 在 SMB 协议的基础上发展并扩展到 Internet 上的协议。它和具体的 OS 无关，在 UNIX 上安装 Samba 后可使用 CIFS。

2) NFS(Network File System)即网络文件系统，由 Sun 公司开发，主要用于 UNIX 和类 UNIX 系统，在 Windows 上使用则需要安装客户端软件进行认证时的指令映射。

将 NFS 置于 Windows 上，有两种选择：Microsoft Services for UNIX (SFU)和 DiskShare。CIFS 采用 C/S 模式，基本网络协议：TCP/IP 和 IPX/SPX。

【问题 2】

RAID1 阵列由磁盘对组成，因为需要用作备份，在数据的安全性方面是最好的，但是只能利用磁盘总容量的一半，存储效率只有 50%，存储性能不高。RAID5 是一种存储性能、数据安全和存储成本兼顾的存储解决方案，以 n 块硬盘构建的 RAID5 阵列可以有 $n-1$ 块硬盘的容量，磁盘空间利用率能达到 $(n-1)/n$。在 RAID5 上，读/写指针可同时对阵列设备进行操作，提供了更高的存储性能。

【问题 3】

1. 远程登录到服务器做诊断或配置可以通过 Telnet、SSH、远程桌面等方式。

Telnet 是 C/S 构架的服务，登录后是命令行界面，客户端和服务器间的传输无私密性保护，一般用于管理网络设备(如路由器交换机)、Linux 或 UNIX 服务器主机。

SSH 和 Telnet 类似，但是提供私密性保护。

远程桌面管理，是登录上服务器的图形化界面配置，一般用于登录 Windows 服务器主机，也可以用于登录 Linux 的图形化界面配置，但是需要 Linux 安装桌面组件。

2. 使用命令诊断邮件服务器的网络连接情况，发现网络丢包严重，根据“丢包”的文字描述，应该是 ping 命令。

3. 交换机上某个端口数据流量异常，收发包量很大，可能的原因很多，比如病毒、端口或网卡物理故障(不是彻底损坏)、环路导致广播风暴等，但是只有木马类病毒才会故意隐藏自己而让服务正常，只是可能木马窃取数据占用了大量带宽导致一些异常。而其他故障都会导致服务不正常，所以依据本题文字描述，登录服务器成功，服务正常，综合考虑，病毒的可能性最大。

【问题 4】

本题说的是“网络安全隐患”，关于网络的安全隐患和性能以及可用性一定要区别清楚，负载均衡、流量控制、划分 VLAN 都是性能方面的问题，链路冗余是可用性方面的问题，而防病毒、针对 Web 的安全防护措施才是安全方面的问题，故 B、C、F、G 体现的是关于网络可靠性、可用性的特征。

1.1.3　同步练习

1. 网络开发设计的整个过程分为哪几个阶段？每个阶段各有什么任务？请用流程图的方式说明。

2. 网络工程是一项复杂的系统工程，一般可分为网络规划、网络设计、工程实施、系统测试验收和运行维护等几个阶段。网络规划是在需求分析的基础上，进行系统可行性分析和论证，以确定网络总体方案。网络规划阶段任务完成之后转入下一阶段，即网络设计阶段。

【问题】

(1)　简述网络规划阶段需求分析的方法和解决的问题(控制在 100 字以内)。

(2)　在需求分析过程中应对已有网络的现状及运行情况作调研，如果要在已有的网络上作新的网络建设规划，如何保护用户已有投资(控制在 100 字以内)？

1.1.4　同步练习参考答案

1. **答案：**

网络开发的过程一般分为 5 个阶段，具体流程图如图 1-3 所示。

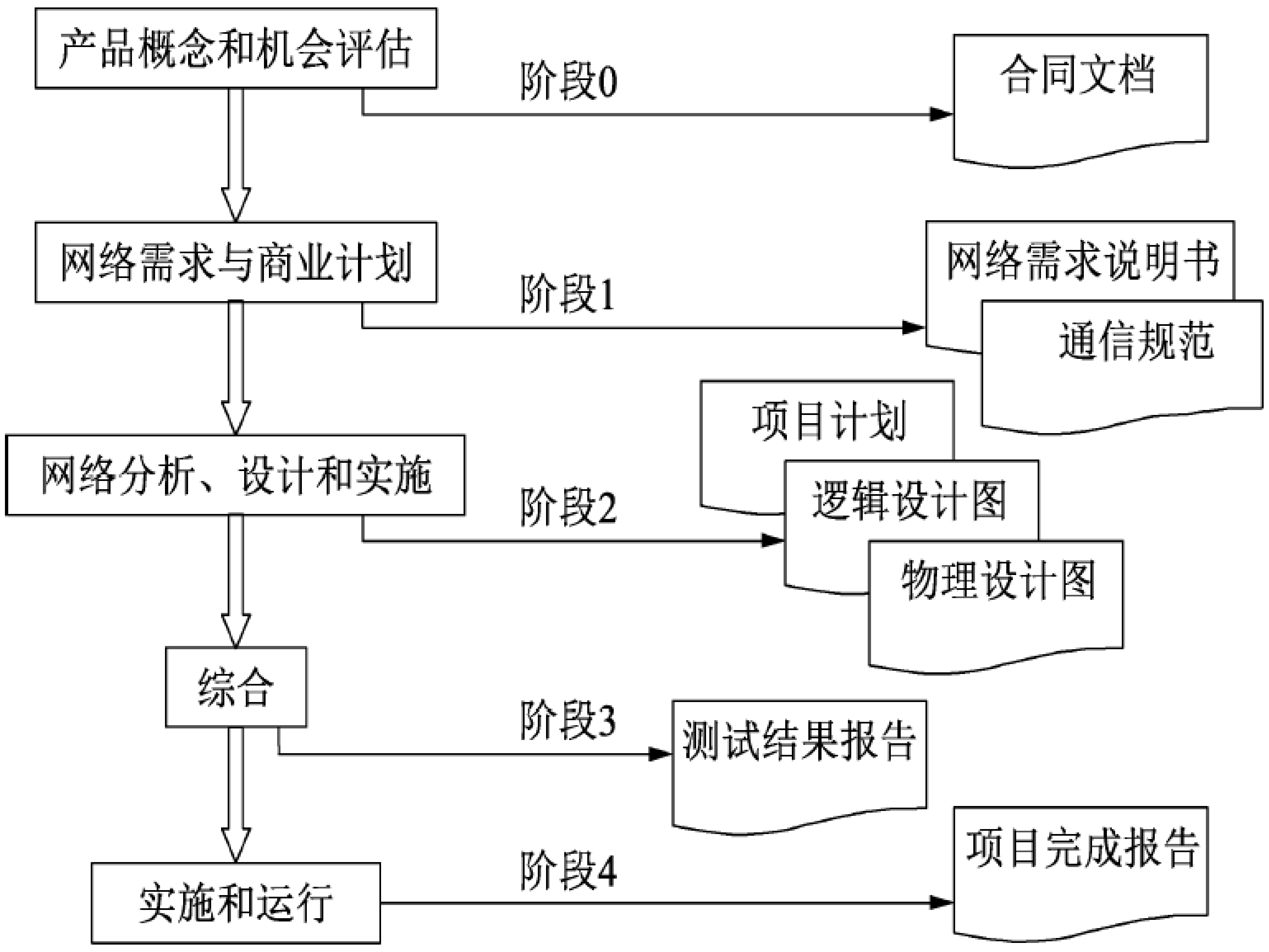


图 1-3　网络开发流程图

2. **答案：**

(1) 先采用自顶向下的分析方法，调查用户单位建网的背景、必要性、上网的人数、信息量等，从而确定建网目标。接着进行纵向的、深入的需求分析和调研，为网络设计提供依据。

(2) 在设计新系统时要充分考虑利用已有系统的资源，让原有系统纳入到新系统中运行，不要“推倒重来”，也可以把已有系统的设备降档次使用。

1.2　网络系统的设计

1.2.1　考点辅导

1.2.1.1　网络设计的基本原则

网络系统性能要求高、技术复杂、涉及面广，在其规划和设计过程中，为使整个网络系统更合理、更经济、性能更好，需要遵守以下设计原则：性价比高；统一建网模式；统一网络协议；保证可靠性和稳定性；保证先进性和实用性；具有良好的开放性和扩充性；在一定程度上保证安全性和保密性；具有良好的可维护性等。

由于不同单位的网络发展水平和应用需求差异很大，而且网络的组网方法和备选设备种类繁多，因此设计时必须根据具体情况进行规划。

1.2.1.2　收集信息

在网络开发过程中，一旦设计者了解网络需求之后，便可进入逻辑网络设计阶段。进入这一阶段的前提是设计者必须有详尽的需求报告和通信规范。

在网络设计的初始阶段，网络设计人员首先需要对用户的需求了如指掌，然后着手进行网络设计前的准备工作。准备工作首先从收集信息(这些信息包括技术层面的和产品层面的)开始，收集信息一定要以满足用户需求为目标，为网络设计和实施服务。

收集信息的途径有很多种，主要有以下几个。

- 通过参观访问其他单位获得。
- 通过厂商资料和宣传品获得。
- 通过 Internet 获得。
- 通过投标公司获得。
- 通过其他渠道获得。

对于收集到的信息需要分类整理，参照需求分析说明书找到可靠的且满足需要的技术、产品和设备，然后进一步分析研究。

1.2.1.3　采用的技术和产品设备的比较研究

任何设计都需要权衡，其中最常见的是成本与性能的权衡。如果要增强性能，成本就会明显上升。在考虑成本时，设计者不仅要考虑运行的成本，还要考虑实施网络的成本。图 1-4 说明了技术选择与成本之间的关系。

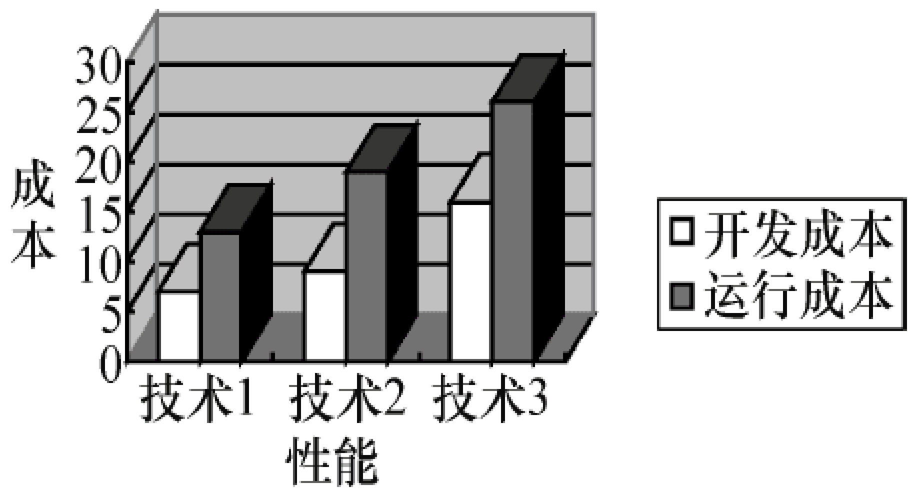


图 1-4　成本/性能示意图

根据需求收集阶段初期收集到的基本需求，可以预测项目的成本，同时也可确定开发成本和运行成本的阈值。在选择技术时，设计者通常也会提供备选的技术及相关的成本，选择的结果一般会超出所确定的水平。给定一个设计目标时，设计者必须考虑以下方面。

- 最低的运行成本。
- 最少的安装费用。
- 最高的性能。
- 最大的适应性。
- 最大的安全性。
- 最高的可靠性。
- 最短的故障时间。

以上目标不可能同时达到，需要仔细权衡。其中技术上的考虑处于核心地位，技术上的考虑包括后台通信、连接类型和可伸缩性等方面。

1. 后台通信

后台通信通常是指广播通信，与应用间的通信不同，它是发生在网络上的通信。考虑后台通信是因为它可能会大大增加网络的容量要求。在典型的情况下，后台通信占全部通信的 5%～20%。

通常遇到的后台通信都是基于路由广告协议(Routing Advertisements Protocol，RAP)和服务广告协议(Service Advertisements Protocol，SAP)。在网络上向其他设备做服务广告的服

务器、路由器和打印机将产生这种类型的通信。如果网络协调不当，后台通信就会在整个网络通信中占很大一部分。

2. 连接类型

连接类型是逻辑设计时必须考虑的另一个问题。在无连接和面向连接的协议间需要一个权衡。有些协议，如 IP 协议是无连接的，在这类协议中，不用花时间来建立虚拟电路，只需简单地通过网络来发送分组。用无连接协议传送信息比起面向连接的协议来说，每个分组的系统花费都要多一些。

面向连接的协议(如 ATM)需要花费较长时间来建立连接。一旦建立起了连接，通信的效率就会高许多。面向连接的协议通常同时提供多层次的服务，当应用需要以相同的速率发送大量的信息时最适合使用面向连接的协议。如果应用是突发的而且不需要多层次服务，则用无连接协议最合适。

3. 可伸缩性

设计者同样需要考虑网络的可伸缩性，即考虑现在以及将来网络所需的容量。容量设计必须易于调整以适应单位、应用以及网络的适当增长。例如，当设计者实施以太网接口卡(NIC)和非屏蔽双绞线(UTP)连接时，即使只实现 10 Mbps 的以太网，也可能选择购买 10/100 Mbps 的网卡和 5 类线。这样做，不更换接口卡和线缆平台就能升级到百兆。

要想作出具体的技术选择，需要设计者详细考虑每种方法的优缺点。考虑的不同技术类型和重点内容如下。

- 物理层。
- 网络互联。
- 逻辑网络图。
- 虚拟网策略。
- 现代广域网技术。
- 网络管理。
- TCP/IP 地址设计。
- 网络安全。
- 防火墙。
- 备选设计。

1.2.1.4 确定连接

除了考虑各种类型的网络的传输特性及优缺点外，还需要考虑在实际网络环境中如何评估各类介质。以下列举了必须要考虑的主要环境因素，并对不同的条件推荐了适当的传输介质。

1) 高 EMI 或 RFI 区域

如果环境内拥有许多电能源，应尽可能使用抗噪性最好的介质。Thick Ethernet(粗缆以太网)和光缆在目前是抗噪性最好的介质。

2) 拐角和狭窄空间

如果环境要求电缆在拐角处弯曲或穿过狭窄空间，应该尽可能使用最灵活的传输介质，如 STP 和 UTP。

3) 距离

如果环境要求远距离传输，应考虑光缆或无线介质，也可以使用双绞线或同轴电缆，但它们更易受衰减和干扰的影响，同时需要中继器。

4) 安全性

如果某个机构对传输安全性要求较高，应选择具有最高安全性的传输介质，光缆和红外介质对这种环境都是很好的选择。

5) 既有体系结构

如果为一个已有的电缆设备增加电缆，应考虑它将如何与已有电缆设备相互作用以及两者之间所需的连接性硬件。选择的介质应与机构以前安装的设备相适应。

6) 发展

应弄清本单位准备如何扩展网络，以及在设计布线时是如何考虑将来的应用、通信业务和地理扩展等问题的，所选的介质应该能适应机构的需求。

1.2.1.5 确定节点

节点是网络中功能相对独立的部分，它可以发送、接收或转发、处理并存储数据，它可能是一台用户终端或服务器，也可能是一个集线器、交换机或路由器等。对于网络设计和规划中需要多少个节点、它们应该如何分布在不同的地理位置、每个节点的处理能力是多少等问题都必须有明确的答案。这就需要网络设计人员综合考虑多种因素，如用户需求、3～5 年后的发展情况、现有网络资源的利用、保证可靠性而采取的冗余措施等。

1.2.1.6 确定网络的性能

网络作为一个系统来看，其性能取决于多种因素，主要包括构成网络的各个部件的性能。网络的性能包括以下 6 个方面。

- 响应时间、延迟和等待时间。
- 利用率。
- 带宽、容量和吞吐量。
- 可用性、可靠性和可恢复性。
- 冗余度、适应性和可伸缩性。
- 效率与费用。

确定网络的性能就是要针对每一种性能选取适当的指标，以保证在网络工程施工后期测试时有据可依，为此，需要评判建成的网络是否满足性能设计要求。

总的来说，网络的性能与网络的投入成正比，即选用的组网设备和部件越好，整个网络的性能就越好。但不同的单位有不同的需求，需要在性能和投入两者之间找到一个平衡点，力争做到投入少、性能好。

1.2.1.7 确定可靠性措施

对于一个网络系统来说，可靠性就是对应用程序和数据的有效支持。在实际应用中，提高网络可靠性的可行方法是消除故障孤点，特别是单点故障。

1. 可靠性设计的内容

可靠性设计包含以下 3 方面的内容。

(1) 物理可靠，指系统对关键硬件设备(如 CPU、存储介质等)损坏，不可预见性灾难(如地震、飓风、陨石、强磁场等)，硬件、数据库及服务资源等破坏的耐受能力。

(2) 逻辑可靠，包含操作系统可靠、数据库管理系统可靠和应用程序可靠等。

(3) 健壮性，指系统在故障情况下恢复正常的难易程度。

对关键硬件设备的损坏，通常采取一定程度的容错措施来应对。根据经验，系统最可能出现的故障原因依次为电源故障、雷击、线路连接和火灾失效等。

2. 广域网的可靠性设计

广域网的可靠性包括冗余的广域网线路及其所带来的额外开销。一种主要的方法是连接备份线路，这样可以避免重复路由的保持和再计算。例如，路由器通过 DDN/Frame Relay(数字数据网/帧中继)连接主干的通信线路，当主干线路出现故障时，路由器可以自动通过 PSTN(公共交换电话网络)或 ISDN(综合业务数字网络)拨入中心路由器。

广域网的可靠性设计包括线路的备份和中心路由器的备份。系统中两个以上部件出现故障时，系统能够自动地在数秒内切换到备份部件上，而无须人工干预。

3. 通信设备的可靠性设计

随着租用线路服务可靠性的增强及其 ISDN/PSTN 后备技术的成熟，系统的可靠性已经在很大程度上转移到了通信设备连接的可靠性上。

防止通信设备损坏对网络造成不良后果的较好解决方案就是使用双电源和双路供电。例如，中心路由器可以采用 Cisco 公司的高性能大型路由器 7204(Cisco 7204 路由器具有双电源容错系统，并且具有端口容错等安全措施来保证系统的稳定运行)。

4. 局域网的可靠性设计

随着通信线路和通信设备的可靠性提高，系统的可靠性已经在很大程度上转移到了局域网连接的可靠性上。一个很好的解决方案就是使用双局域网服务。主机与两个局域网适配器相连，每个适配器连接到一个单独的集线器或交换机上，这样主机与主干交换设备之间的关键连接就具有较高的可靠性。

网络设计人员应根据组网需求，选择符合要求的可靠性结构和策略。

1.2.1.8 网络设备的选择

网络设备质量的高低直接影响着网络系统的性能。选择设备时，首先必须制定选择标准，即根据用户单位实际需要制订成本、性能、容量、处理量、延迟等指标和浮动范围，在能够满足需求的情况下，没有必要一味地求高求贵，而要参照产品的性能价格比来决定。

在设备到达现场时，需要检验其标称性能参数与既定标准的一致性，看是否有性能不达标的产品存在，以免设备投入运行后影响整个系统的性能。

设备安装到位且初步调试通过后，还需要采取专门的测试手段对关键设备进行高级测试，只有当设备在实际环境中的性能表现和与其他设备的兼容性和互联性完全符合标准后才能通过验收。

在选择产品时，除了要求产品支持应用需求之外，还建议考虑如下因素：选用符合工业标准的流行产品(保证产品的兼容性、可靠性和可扩充性)，具有较多的工具软件和应用软件支持，具有进一步开发的接口，具有完整的资料说明等。

作为网络工程，被选择的产品主要包括传输介质、网络接口、互联部件、网络服务器以及通信协议和应用软件等。

1. 传输介质

传输介质是网络的最基本部分，用于在用户设备之间传输信号。选择传输介质时，应当考虑如下因素。

- 安装特性：包括单段介质的最大长度、网络的覆盖范围、铺设时允许的最小弯角和最大直径等。
- 连接性：包括网络拓扑、可支持的连接数据等。
- 容量及性能：包括可使用的带宽、支持的逻辑信道数、每个信道可以支持的最大传输速率等。
- 防护性能：包括电气干扰与噪声、物理损害、安全性等。
- 价格：介质的价格。

目前可以选择的介质类型包括以下几类。

- 无屏蔽双绞线：支持点到点连接(包括环形)，价格较低，用于计算机联网的双绞线应为 3 类线以上。
- 屏蔽双绞线：支持点到点连接(包括环形)，仅用于电磁干扰较严重的环境，价格适中。
- 基带同轴电缆：支持总线连接(包括环形)，价格适中。
- 宽带同轴电缆：支持总线连接(包括环形)，价格略高。
- 光纤：支持点到点连接(包括环形)，价格偏高。

随着结构化布线技术的推广以及多介质应用的增多，双绞线和光纤成为组网的主要传输介质。

需要指出的是，传输介质的选择应当具有足够的超前意识，因为传输介质的布放一般会对建筑物的本身造成影响，因此应当尽可能避免因设备的更新换代和升级而改变传输介质。

2. 网络接口

网络接口的用途是将用户设备接入网络，网络接口通常以网络适配卡的形式出现。使用不同的传输介质和采用不同的访问介质控制方法时，要求使用不同类型的网络适配卡。

目前，常用的网络适配卡包括以下几种。

- 以太网卡：支持总线方式，具有不同的速率和工作方式的接口，可以连接双绞线、同轴电缆和光纤。
- ARCnet 网卡：支持总线方式，具有不同的接口，可以连接双绞线、同轴电缆，常用于生产控制环境。
- 令牌环卡：支持环形结构，连接双绞线。
- X.25 卡：支持用户终端接入 X.25 网络，连接双绞线。

- ATM 适配卡：支持用户设备接入 ATM 网络，连接光纤。
- FDDI 适配卡：支持用户设备接入 FDDI 网络，连接光纤或者铜芯电缆。

3. 互联部件

互联部件主要用于网络的扩展或者网络的互联。为了结构化布线的需要、减少设备之间的干扰和方便系统升级，局域网组建建议采用集线器方式。常用的互联部件包括以下几个。

- 集线器：有一般集线器和智能集线器之分，主要用于连接节点，所有端口共享链路带宽。
- 交换器(交换式集线器)：一种采用线路交换技术的集线器，具有端口链路分隔的特征，常用于连接网段或者相同类型的局域网。
- ATM 交换机：可以直接连接节点或者和其他 ATM 交换机连接，形成 ATM 网络。
- FDDI 集中器：可以直接连接节点或者和其他 FDDI 集中器等连接，形成 FDDI 网络。
- 路由器：常用的路由器包括远程访问路由器(支持远程用户通过拨号/专线方式访问内部网)、局域网/广域网路由器(支持用户通过各种公共网络进行互相访问)。

目前较高档的互联部件均采用了模块化结构，允许用户根据具体的应用需求选择和插入不同的模块。

选用交换器或者交换机时，应当注意其内部的交换结构；选用路由器时，应当考虑采用的路由算法，以及支持分组过滤的安全策略。

4. 网络服务器

网络服务器通常是小型机或者高档微机，它通过网络适配卡接入网络，向用户提供各种共享服务，如文件共享、打印共享、通信共享、电子邮件和 WWW 服务等。网络服务器可根据服务的类型，扩充不同的设施，例如，文件服务器要求较大容量的硬盘和高速缓冲区支持，打印服务器应当配置打印机。原理上，一台服务器可以提供多种应用服务，但在实际应用中，尤其是从安全和可扩展的角度出发，仍然建议在经费许可的前提下，根据应用服务划分和配置多台服务器。

5. 通信协议和应用软件

通信协议和应用软件的选择除了要满足具体的应用需求之外，还应考虑开放性，不仅要保证和不同厂家的不同产品之间的相互操作，还应兼顾和其他相关部门之间的关系(例如，对于数据库管理系统的选择应当兼顾与上级部门选择的一致性)。设计时应当允许三个阶段的并存，即原有的网络协议软件可能是“封闭”的，仅适合于连接同一厂家的产品(大多数生产控制系统具有这样的特性)；现行的网络协议软件要求是“开放”的，此时的整个网络系统为“混合型”的；将来的系统是完全“开放”的。

需要指出的是，任何一个系统(包括网络系统)都具有一定的生命周期，因此，应当从系统的功能、技术和效益等方面，对所设计的系统作出正确的系统生命周期估计。就现阶段而言，TCP/IP 协议应是通信协议选择的主流。

产品选择阶段的工作应由专业技术人员完成，或者直接委托供应商和公司完成。采用委托方式时，应在企业代表的全面控制下进行。

在选择供应商时，建议考虑如下因素：资金相对雄厚且具有良好的业绩，可以提供可

靠的产品，能够提供可靠的服务质量，尤其是售后服务质量好的公司。组建网络的最终目的是应用，因此，具有相关拳头产品或者应用软件开发能力较强也可成为选择供应商的指标之一。

1.2.1.9　设计管理

网络设计方案管理的任务包括设计复查、设计验证、设计确认和设计变更。

(1)　设计复查：项目计划中规定，对设计结果必须复查且对复查应留有备案。

(2)　设计验证：在项目计划中，经过设计复查和测试后，设计验证才能完成。需要按照复查结果验证设计输出是否符合设计输入的需求，如果任一部分的设计未通过验证，必须进行设计修复。

(3)　设计确认：设计确认就是要确保产品遵照产品需求说明书进行设计。产品的质量保证依赖于用来进行验证、确认和控制的测试工具，以及在确认及验证阶段使用的程序。

(4)　设计变更：设计变更需要修改相关设计文档并备案。

1.2.1.10　新网络业务运营计划

新网络运营过程一般是公司业务由旧的网络向新的网络迁移的过程。旧有业务应用适合于原有网络，而新系统由于在功能、性能、技术等方面都与旧的网络系统存在较大差异，因而对业务系统的支持也不同，直接将旧的业务系统迁移到新系统上是不太现实的，新系统的使用往往与新的业务系统配套。

在向新系统升迁前，应该周密计划，需要仔细考察新、旧系统的差异，分析升迁对用户造成的影响并及时通知他们。考虑到用户不能很快接受并适应新系统，升迁前还需要对他们进行系统的业务操作培训。如果一个单位的业务应用分为若干部分，也可以按照先易后难的顺序，一个部分一个部分地迁移到新系统，逐步积累新系统的使用经验，为后续部分的升迁作准备。

在整个升迁过程中，要及时做好系统备份，包括旧系统的备份，以便在新系统不可用时能够及时恢复到旧系统，保证业务正常开展。迁移完毕后，还需要对新业务系统进行测试，检查其对于设计目标的可满足性。新系统迁移成功后，对旧系统应采取措施妥善处理。

所有这些工作都将在网络系统实施阶段完成，因而在设计阶段应该针对每一个环节制订详细的计划，以便以后按计划实施。

1.2.1.11　设计方案测试

测试一个网络、预测和衡量网络性能是一门科学。没有两个完全相同的系统，因此对测试方法和测试工具的正确选择需要具有一定的创造性，还需要对所测试的系统有透彻的理解。

1. 测试原型网络系统的方法和工具

根据所要测试项目的应用目的正确选择测试方法和测试工具，通常包括以下内容。

- 验证该设计是否满足商业技术目标。
- 验证所选择的局域网技术、广域网技术和设备是否合适。
- 验证服务提供者是否能够提供要求的服务。
- 找出系统瓶颈或连通性问题。

- ◆ 测试网络冗余。
- ◆ 分析网络链路故障对性能的影响。
- ◆ 确定必要的优化技术，需满足的性能和其他技术目标。
- ◆ 分析网络链路和设备升级对性能的影响。
- ◆ 证明该设计优于其他竞争方案。
- ◆ 通过一个“验收测试”以获得进行下一步的网络实现。
- ◆ 发现可能妨碍执行的风险，并拟定相应的补救措施。
- ◆ 决定还需要多少其他测试。

如果网络设计方案中选用的设备不是全新的设备，也即该设备或相应的组网方案已经得到应用，上述测试内容就可以大大简化。一个比较简单的方法是，考查采用类似方案的现有网络系统，如果可能，可以考虑在不影响该网络业务正常运行的前提下，支付必要的费用，对该网络进行所需要的测试。这种方法的优点是：可以节省大量的资金和时间，与实际结合比较紧密。

如果采用的是全新的设备和网络设计方案，也应该要求设备厂商进行必要的测试或提供尽可能全面的测试资料，特别是第三方的权威测试结果报告，以降低测试费用。

2. 建立和测试原型网络系统

原型网络系统是新系统的一个初始实现，为最终完成系统提供了一个样板，可以帮助网络设计者验证所设计的新系统的功能和性能。

建立和测试原型网络系统能否顺利实施取决于所能得到的资源支持，包括人工、设备、资金和时间等。完成有效的测试需要有足够的资源，但是如果资源消耗过多会导致项目预算超支、时间过长或对用户产生不利影响。

以下就是建立和测试原型系统常用的 3 种方法。

- ◆ 在实验室中建立和测试网络。
- ◆ 与正在运行的网络集成，利用空闲时间进行测试。
- ◆ 与正在运行的网络集成，在正常工作时间内进行测试。

一旦网络设计方案得到认可，剩下的关键问题就是对原型网络系统进行测试，以考查可能出现的设计瓶颈。这种测试可以在空闲的时间进行，但最终的测试必须放在正常的工作时间内进行，从而能够在正常负载的情况下对系统进行评估。

在确定了原型系统的测试范围后，应该制订测试计划，说明如何测试该原型系统。

测试计划涉及的内容应当包括以下方面。

- ◆ 测试目标和验收标准。
- ◆ 测试的种类。
- ◆ 网络设备和所需的其他资源。
- ◆ 测试脚本。
- ◆ 测试项目的时间划分和阶段划分。

测试计划执行的过程主要是按测试脚本执行并将工作归档。由于在编写测试脚本时不可能把所有突发情况和可能出现的各种问题都考虑到，因而无法按部就班地执行测试计划。所以，在测试计划执行的过程中对日志记录进行维护就显得非常重要。

日志记录应当包括测试数据、测试结果以及每日活动记录。每日活动记录用来记载测试记录，包括对测试脚本或设备配置所做的改变、遇到的问题和对引起这些问题原因的推测。这些推测记录在分析测试结果时往往能够发挥重要的作用。

3. 网络测试工具

网络设计的测试工具一般包括以下几个。

◆ 网络管理和监控工具。
◆ 建模和仿真工具。
◆ 服务质量和服务级别管理工具。

1.2.1.12　设计评审

对于按照以上规范提出的网络逻辑设计方案，必须得到批准后才能够实施。

先交由单位组建的网络评审委员会讨论，审查该方案是否满足本单位对新网络的各种类型的需求，网络规划是否合理，使用的技术是否先进，选择的设备厂商是否信誉良好，网络的实施成本是否在单位的预算之内等，不同的单位可能有不同的审查准则。在所有条件均满足之后，网络设计方案才能得到批准。

批准时，需要由单位的管理部门、MIS(管理信息系统)职员和咨询公司代表签字。

1.2.2　典型例题分析

例 1　阅读以下说明，回答问题。(2015 年上半年下午试题一)

【说明】

某企业网络拓扑图如图 1-5 所示。

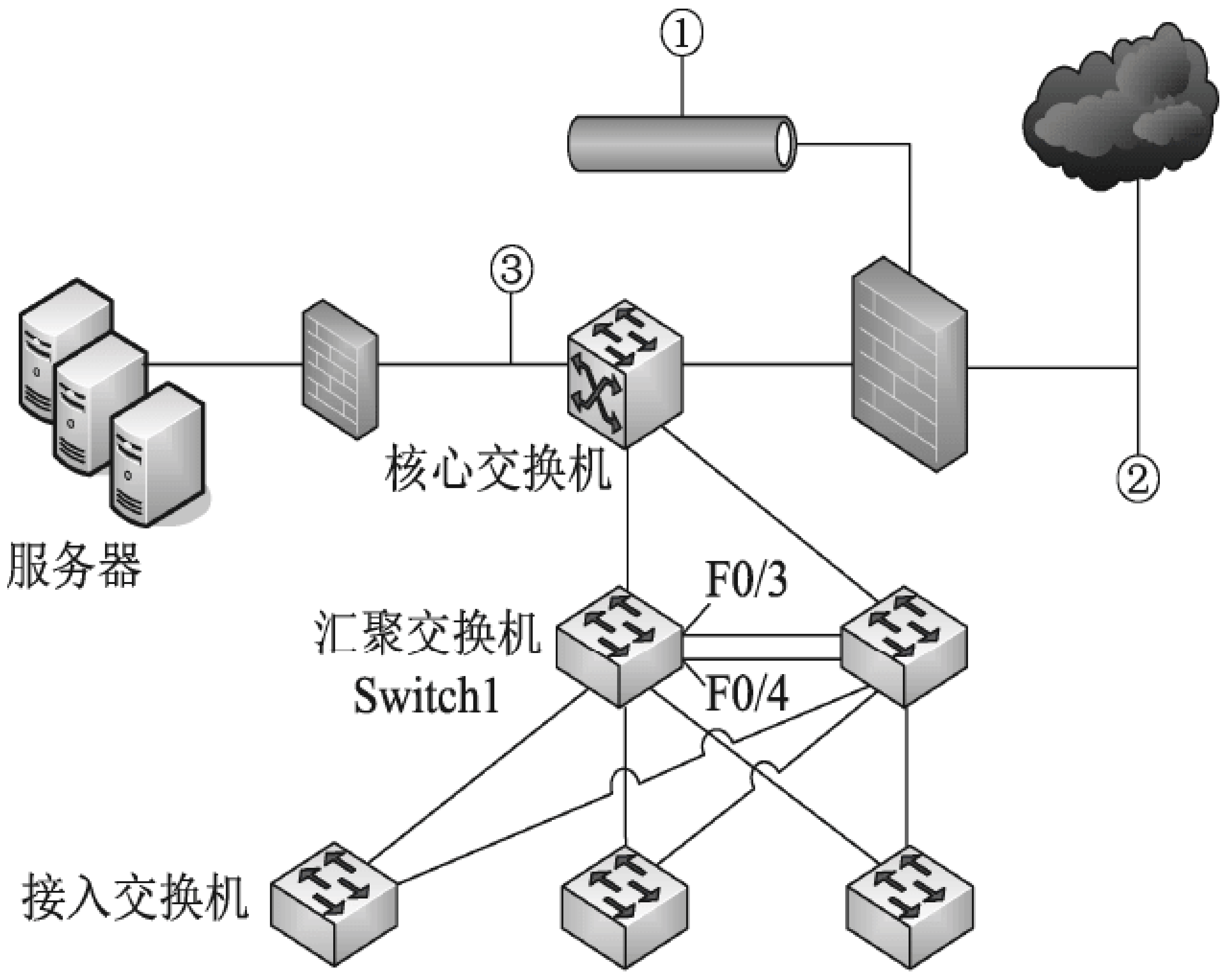


图 1-5　某企业网络拓扑图

工程师给出了该网络的需求：

1. 用防火墙实现内外网地址转换和访问控制策略；
2. 核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；
3. 接入层到汇聚层采用双链路方式组网；

4. 接入层交换机对地址进行 VLAN 划分；

5. 对企业的核心资源加强安全防护。

【问题 1】(4 分)

该企业计划在①、②或③的位置部署基于网络的入侵检测系统(NIDS)，将 NIDS 部署在①的优势是 (1) ；将 NIDS 部署在②的优势是 (2) 、 (3) ；将 NIDS 部署在③的优势是 (4) 。

(1)～(4)备选答案：

A. 检测外部网络攻击的数量和类型

B. 监视针对 DMZ 中系统的攻击

C. 监视针对关键系统、服务和资源的攻击

D. 能减轻拒绝服务攻击的影响

【问题 2】(4 分)

OSPF 主要用于大型、异构的 IP 网络中，是对 (5) 路由的一种实现。若网络规模较小，可以考虑配置静态路由或 (6) 协议实现路由选择。

(5) 备选答案：A. 链路状态　　B. 距离矢量　　C. 路径矢量

(6) 备选答案：A. EGP　　B. RIP　　C. BGP

【问题 3】(4 分)

对汇聚层两台交换机的 F0/3、F0/4 端口进行端口聚合，F0/3、F0/4 端口默认模式是 (7) ，进行端口聚合时应配置为 (8) 模式。

(7)、(8)备选答案：

A. multi　　B. trunk　　C. access

【问题 4】(6 分)

为了在汇聚层交换机上实现虚拟路由冗余功能，需配置 (9) 协议，可以采用竞争的方式选择主路由设备，比较设备优先级大小，优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文，则将自己的状态转为 (10) 。

为了避免二层广播风暴，需要在接入与汇聚设备上配置 (11) 。

(10)、(11)备选答案：

A. Master　　B. Backup　　C. VTP Server　　D. MSTP

【问题 5】(2 分)

阅读汇聚交换机 Switch 1 的部分配置命令，回答下面的问题。

```
Switch 1(config)#interface vlan 20
Switch 1 (config-if)#ip address 192.168.20.253 255.255.255.0
Switch 1(config-if)#standby 2 ip 192.168.20.250
Switch 1(config-if)#standby 2 preempt
Switch 1(config-if)#exit
```

VLAN20standby 默认优先级的值是 (12) 。

VLAN20 设置 preempt 的含义是 (13) 。

答案：

【问题 1】

(1) B　　(2) A　　(3) D　　(4) C

【问题 2】

(5) A　　　(6) B

【问题 3】

(7) C　　　(8) B

【问题 4】

(9) HSRP　　(10) A　(11) D

【问题 5】

(12) 100　　(13) 设置抢占模式

解析：

【问题 1】由图 1-5 可知，①位于 DMZ 区，所以可以监视针对 DMZ 中系统的攻击。②连接外网，所以可以检测外部网络攻击的数量和类型、减轻拒绝服务攻击的影响。③位于内网服务器区域，所以可以监视针对关键系统、服务和资源的攻击。

【问题 2】OSPF 属于链路状态路由协议。网络规模小，可采用 RIP 路由协议，而 EGP 和 BGP 属于外部网关路由协议。

【问题 3】交换机默认端口的模式为接入模式 access，对汇聚层交换机进行端口聚合时，一般配置为 trunk 模式。

【问题 4】汇聚交换机采用虚拟路由冗余，目的是当一台汇聚交换机出现故障时，启用备份线路。根据设备情况可以采用虚拟路由器冗余协议(VRRP)或热备份路由器协议(HSRP)。

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

【问题 5】

```
Switch1(config)#interface vlan 20    //进入 VLAN20 虚接口
Switch1(config-if)#ip address 192.168.20.253 255.255.255.0 //配置 IP 地址
Switch1(config-if)#standby 2 ip 192.168.20.250   //配置备份组 2 的虚拟 IP
Switch1(config-if)#standby 2 preempt     //配置抢占功能
Switch1(config-if)#exit
```

默认优先级为 100，取值范围为 0～255，值越大，优先级越高。

例 2　【说明】(2014 年下半年下午试题一)

某企业的网络结构如图 1-6 所示。

【问题 1】(6 分)

1. 图 1-6 中的网络设备①应为__(1)__，网络设备②应为__(2)__，从网络安全的角度出发，Switch9 所组成的网络一般称为__(3)__区。

2. 图 1-6 中③处的网络设备的作用是检测流经内网的信息，提供对网络系统的安全保护。该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为__(4)__，其连接的 Switch1 的 G1/1 端口称为__(5)__端口，这种连接方式一般称为__(6)__。

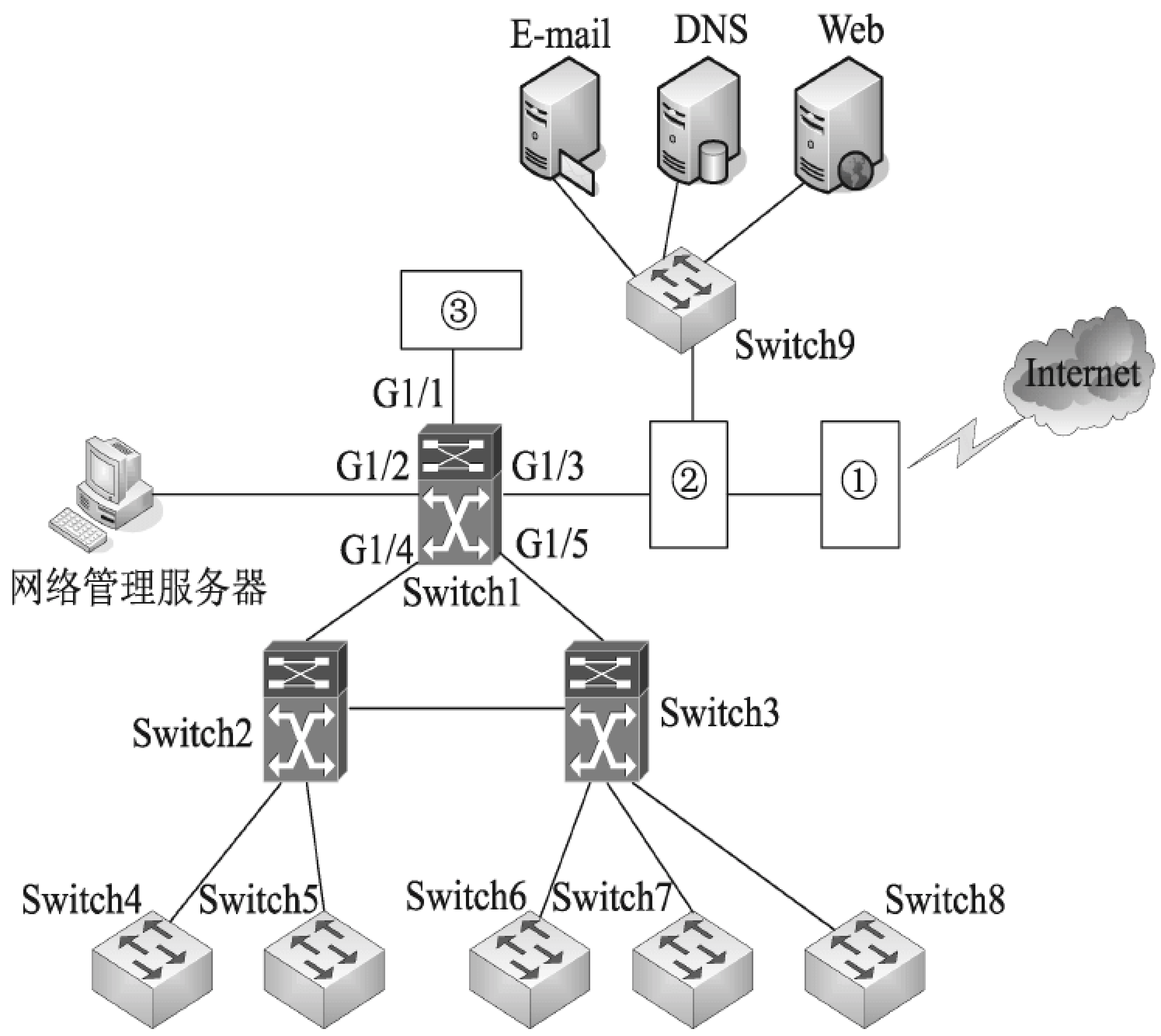


图 1-6　某企业的网络结构

【问题 2】(5 分)

1. 随着企业用户的增加，要求部署上网行为管理设备，对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在图 1-6 中的__(7)__和__(8)__之间比较合理。

2. 网卡的工作模式有直接、广播、多播和混杂四种模式，缺省的工作模式为__(9)__和__(10)__，即它只接收广播帧和发给自己的帧。网络管理机在抓包时，需要把网卡置于__(11)__模式，这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【问题 3】(5 分)

针对图 1-6 中的网络结构，各台交换机需要运行__(12)__协议，以建立一个无环路的树状网络结构。按照该协议，交换机的默认优先级值为__(13)__，根交换机是根据__(14)__来选择的，值小的交换机为根交换机；如果交换机的优先级相同，再比较__(15)__。当图 1-6 中的 Switch1—Switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 Switch1—Switch3 上使用__(16)__功能。

【问题 4】(4 分)

根据层次化网络的设计原则，从图 1-6 中可以看出该企业网络采用了由__(17)__层和__(18)__层组成的两层架构，其中，MAC 地址过滤和 IP 地址绑定等功能是由__(19)__完成的，分组的高速转发是由__(20)__完成的。

答案：

【问题 1】

(1) 路由器　(2) 防火墙　(3) DMZ　(4) IPS　(5) 镜像　(6) 旁路模式

【问题 2】

(7) 防火墙　(8) SW1　(9) 直接　(10) 广播　(11) 混杂

【问题 3】

(12) STP　(13) 32768　(14) 交换机 ID　(15) MAC 地址　(16) 上行速链路

【问题 4】

(17) 核心层　(18) 接入层　(19) 接入层　(20) 核心层

解析：

【问题 1】网络设备①接入 Internet 应为路由器，那么设备②即为防火墙，Switch9 所接区域应为 DMZ 区。

根据该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报，可判断设备③为 IPS，则其连接的 G1/1 端口称为镜像端口，这样的连接方式为旁路模式。一般 IPS 以串接的方式接入网络，但是此题的部署方式并不常规，根据题意预先对入侵活动和攻击性网络流量进行拦截，避免造成损失来判断应为 IPS。

【问题 2】上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析，上网行为管理设备的位置应该在防火墙和 SW1 之间。

网卡具有如下几种工作模式。

(1) 广播模式(Broad Cast Model)：它的物理地址(MAC)是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

(2) 多播传送(MultiCast Model)：多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

(3) 直接模式(Direct Model)：工作在直接模式下的网卡只接收目地址是自己 MAC 地址的帧。

(4) 混杂模式(Promiscuous Model)：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接受同一网络内所有站点所发送的数据包，这样就可以达到对于网络信息监视捕获的目的。

【问题 3】生成树算法的网桥协议 STP(Spanning Tree Protocol)，通过生成树来保证一个已知的网桥在网络拓扑中沿一个环动态工作。

STP 的算法分为 3 个步骤：

(1) 选择根网桥(Root Bridge)，依据：网桥 ID(BID)= 网桥优先级+网卡的 MAC 地址，其中网桥 ID 是唯一的，以及选择交换网络中网桥 ID 最小的交换机成为根网桥。注意：优先级取值范围为 0～65535，缺省值为 32768。

(2) 选择根端口(Root Ports)，依据：到根网桥最低的根路径成本，直连的网桥 ID 最小，直连的端口 ID 最小。注意：端口 ID=端口优先级+端口编号，端口优先级范围为 0～255，缺省值为 128。其中根路径成本为：网桥到根网桥的路径上所有链路的成本之和。

(3) 选择指定端口(Designated Ports)。

配置上行速链路，当接入层或汇聚层的交换机主用的上行链路断开的时候，被阻塞的

端口迅速转换到转发的状态，不需要经历侦听和学习状态。

【问题 4】层次化网络模型包括:

(1) 由经过可用性和性能优化的高端路由器和交换机组成的核心层。

(2) 由用于实现策略的路由器和交换机构成的汇聚层。

(3) 通过用以连接用户的低端交换机等构成的接入层。

核心层是网络高速交换的主干，接入层为用户提供了在本地网段访问应用系统的能力，具有过滤 MAC 地址、绑定 IP 地址等功能。

1.2.3 同步练习

【说明】(2014 年上半年下午试题一)

某单位计划部署园区网络，该单位总部设在 A 区，另有两个分支机构分别设在 B 区和 C 区，各个地区之间距离分布如图 1-7 所示。

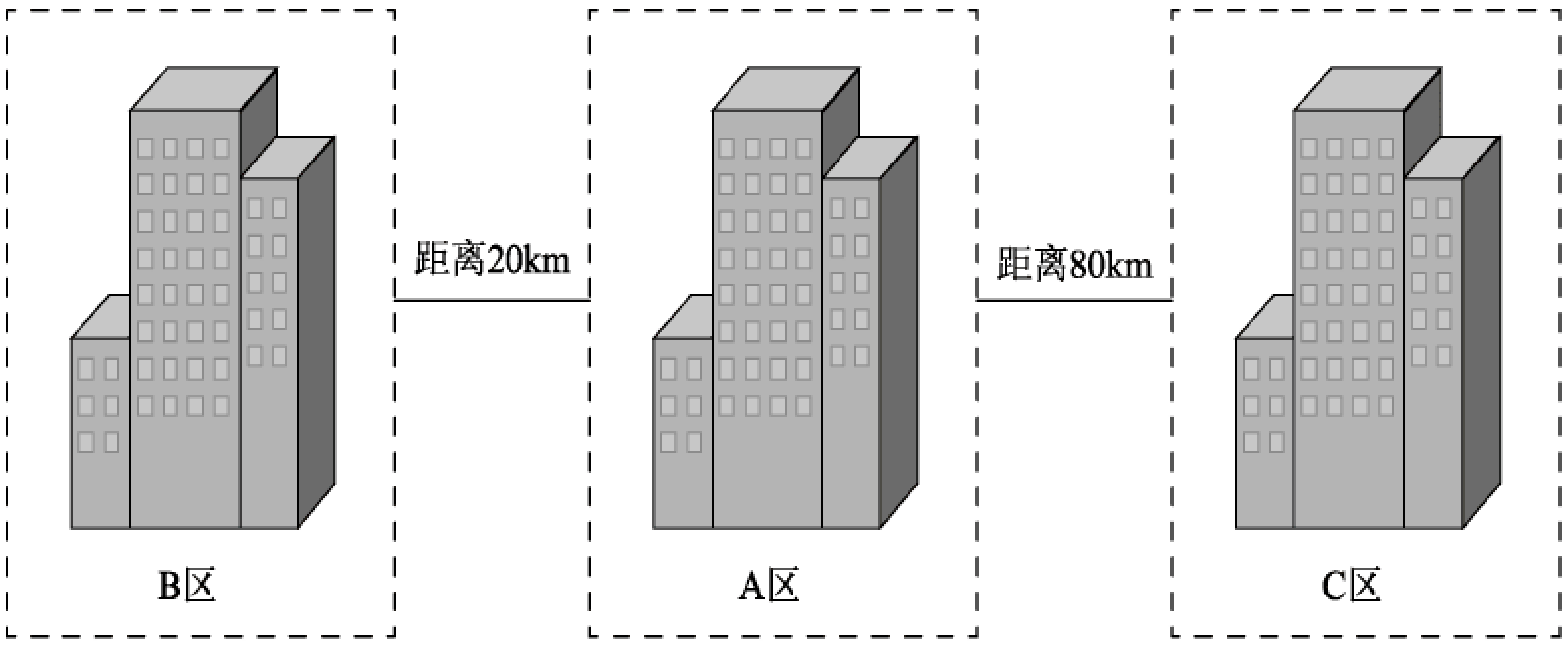


图 1-7 各地区之间距离分布

该单位的主要网络业务需求在 A 区，该网络中心及服务器机房亦部署在 A 区；B 区的网络业务流量需求远大于 C 区；C 区虽然业务流量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互通并且都能够访问互联网，同时基于安全考虑，单位要求采用一套认证设备进行身份认证和上网行为管理。

【问题 1】(6 分)

为了保障业务需求，该单位采用两家运营商接入 Internet。根据题目需求，回答下列问题：

1. 两家运营商的 Internet 接入线路应部署在哪个区？为什么？

2. 网络运营商提供的 MPLS-VPN 和千兆裸光纤两种互联方式，哪一种可靠性高？为什么？

3. 综合考虑网络需求及运营成本，在 AB 区之间与 AC 区之间分别采用上述哪种方式进行互联？

【问题 2】(8 分)

该单位网络部署接入点情况如表 1-1 所示。

根据网路部署需求，该单位采购了相应的网络设备，请根据题目说明及表 1-1，确定表 1-2 所示的设备数量及合理的部署位置(注：不考虑双绞线的距离限制)。

表 1-1　单位网络部署接入点情况

区　域	汇 聚 点	接 入 点	备　注
A	办公楼	124	所有区域采用三层局域网结构部署，其中 A 区采用双核心交换机冗余。所有汇聚点采用单模光纤上联至核心交换机。所有接入交换机采用双绞线上联至汇聚交换机
	资料室	86	
	网管中心	78	
	设计中心	200	
	生产区	115	
B	办公楼	106	
	培训中心	126	
	宿舍	198	
C	办公楼	86	
	营销中心	54	

表 1-2　设备及部署区域

设备类型	设备数量	部署区域
核心交换机	__(1)__	A 区
核心交换机	1	B 区
核心交换机	1	C 区
汇聚交换机	5	A 区
汇聚交换机	3	B 区
汇聚交换机	2	C 区
SFP 单模模块	5	__(2)__ 区
SFP 单模模块	7	__(3)__ 区
SFP 单模模块	22	__(4)__ 区
24 口接入交换机	__(5)__	A 区
24 口接入交换机	__(6)__	B 区
24 口接入交换机	__(7)__	C 区
千兆服务器接入交换机	1	A 区
服务器	3	A 区
服务器	1	__(8)__ 区
认证及流控设备	1	A 区
防火墙	1	A 区

【问题 3】(6 分)

根据题目要求，在图 1-8 的方框中画出该单位 A 区网络拓扑示意图(汇聚层以下不画)。

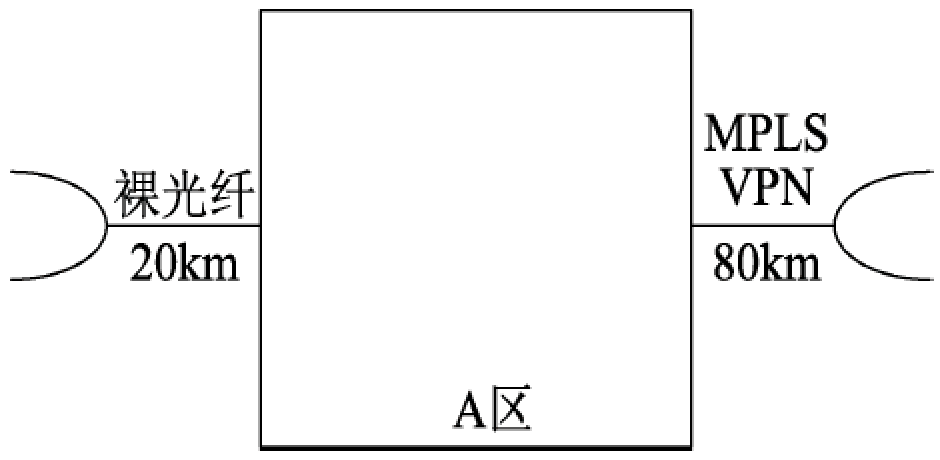


图 1-8　问题 3 图示

1.2.4　同步练习参考答案

答案：

【问题 1】

1. A 区。原因：A 区是网络中心，B 区和 C 区接入 Internet 流量都需要经过 A 区。

2. 裸光纤高。原因：MPLS-VPN 是本地线路走 SDH 专线，链接到运营商的专网 MPLS-VPN。裸光纤是物理层的点对点链接，所以可靠性当然是裸光纤高。

3. AB 区之间用裸光纤，AC 区之间用 MPLS-VPN。

【问题 2】

(1) 2　(2) C　(3) B　(4) A　(5) 27　(6) 19　(7) 7　(8) A

【问题 3】

A 区网络拓扑如图 1-9 所示。

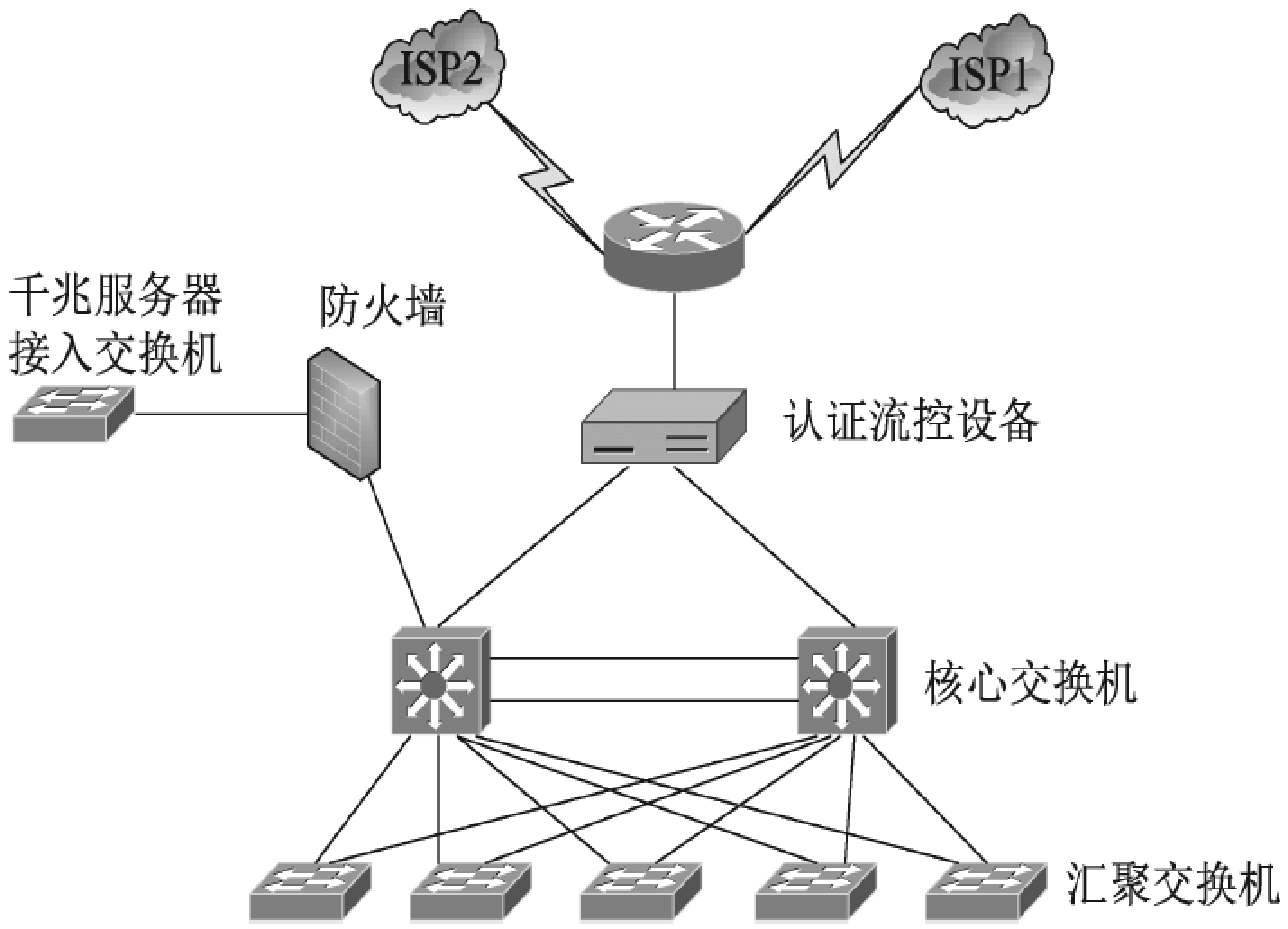


图 1-9　A 区网络拓扑示意图

解析：

【问题 1】

1. A 区是网络中心和服务器机房部署区域，便于维护整个企业网络。两个区域的网络能够互联互通且都能访问因特网，且接入方式部署在中间 A 区，ABC 区之间总体跨越里程距离最短，总体成本最小。

2. MPLS-VPN 是本地线路走 SDH 专线，连接到运营商的 MPLS-VPN 专网。裸光纤是

物理层的点对点连接，所以可靠性当然是裸光纤高。

3. AB 区之间用裸光纤，AC 之间用 MPLS-VPN 方式。因为 B 区的业务流量需求量大于 C 区，因此，需要高带宽。而由于 AC 之间业务流量小，二者相距 80km，如果采用传输带宽远大于 MPLS-VPN 的裸光纤，由于距离较远，会造成过高的成本，所以出于成本考虑，用 MPLS 合适。

【问题 2】

A 区采用双核心交换机冗余，其核心交换机数量为 2 台。A 区汇聚交换机为 5 台，单模光纤双线冗余至核心交换机，对单模模块的数量要求在 10 个以上，考虑到 A 区双核心之间的以太网通道，以及 A 区防火墙、认证与流控设备、出口路由器之间的光纤互联，A 区所需要的光纤模块是最多的。B 区 3 台汇聚交换机，所要求的单模光纤模块数量次之，C 区 2 台汇聚交换机所要求的单模光纤模块数量最少。A 区共 124+86+78+200+115=603 个信息点，每个接入层交换机会用掉 1 个端口连接汇聚层交换机，那么 A 区任何一台 24 口接入层交换机能接主机的端口数量为 23 个，所以 A 区需要的接入层交换机数量为 27 台(603/23≈26.217，向上取整为 27 台)。同理，B 区接入层交换机数量为 19 台，C 区接入层交换机数量为 7 台。路由器作为互联设备，应该放置在 A 区。

【问题 3】

A 区采用双核心交换机，汇聚层可采用单模光纤双线冗余上联至两台核心交换机，核心交换机之间可通过以太网通道技术以提高带宽和链路备份。

核心交换机可直接连入防火墙，防火墙通过千兆服务器接入交换机，保障服务器区域的安全。双核心交换机共两条光纤连接认证与流控设备，最后由认证与流控设备连接出口路由器，出口路由器采用双 ISP 互联方式进入 Internet。

1.3　网络系统的构建和测试

1.3.1　考点辅导

1.3.1.1　安装工作

1. 网络实施过程

网络实施是在网络设计的基础上，进行设备的购买、安装、调试、培训和系统切换等工作。网络实施包括以下步骤。

1)　工程实施计划

安装网络设备之前，需要准备一个工程实施计划，列出需安装的项目、安装费用、安装负责人等，以便控制投资和进度，按进度要求完成安装任务。工程实施计划必须包括网络实施阶段的设备验收、人员培训、系统测试以及网络运行维护等具体事务的处理，必须合理安排工程实施的时间，并充分调动有关人员的积极性。

2)　网络设备到货验收

订购的网络设备到货后，在安装调试之前，必须先进行严格的功能和性能测试，以保

证购买的产品能很好地满足用户的需要。

3) 设备安装

网络系统的工程安装和调试要由专门的技术人员负责。安装项目一般可分为布线系统、网络设备、主机服务器、系统软件、应用软件等几个部分，不同部分应由专门的工程师进行安装调试。

4) 系统测试

系统安装完毕，要进行系统测试。系统测试是保证网络安全可靠运行的基础。

5) 系统试运行

系统调试完毕后，进入试运行阶段。这一阶段的任务主要是验证系统在功能上、性能上是否达到预期目标，若没有达到，则需要不断调整直至达到用户要求。

6) 系统切换

系统经过一段时间的试运行，达到稳定可靠的水平，就可以进行系统切换了。系统切换是指从原有人工或计算机系统上迁移到新平台上工作。具体有三种切换方法：双运行方式(两种运行方式同时运行)、逐步替代法(用新系统逐步替代原有的网络系统)和直接切换法(停止旧系统，启动新系统)。显然，这三种方法的可靠性和成本各不相同，应视具体情况而定。

7) 人员培训

对有关人员的培训是网络建设的重要一环，也是保证业务正常开展的一个重要因素。一个规模大、结构复杂的网络系统往往需要网络管理员来维护网络、协调网络资源的使用。

2. 结构化综合布线系统

结构化综合布线系统(SCS)是一种模块化、灵活性极高的建筑物和建筑群内的信息传输系统。它是一种集成化的通用传输系统，利用双绞线或光缆来传输建筑物内的多种信息。

在现代化的大型建筑中，除计算机网络系统以外，通常还会有电话系统、楼宇控制系统等各种专业布线系统。传统的做法是：为不同的专业系统配置不同的线缆、插座及接头等不同的布线材料来构成各自的网络；连接这些不同网络的插头、插座及配线架互不兼容，只要变动终端机的位置，就得重新布放新的线缆，安装新的插座。在这种传统的布线方式下，因办公室的重新规划及办公设备的变更而导致的布线系统的变更要耗费大量的金钱和时间，同时，对于布线系统的日常维护和管理、故障的检查和排除都不太方便。

为解决传统布线方式中的种种弊端，工业界推出了结构化综合布线系统。SCS 将所有的语音、数据、图像及监控设备的布线组合在一套标准的布线系统上，采用统一的线缆、插头、插座及配线架，当终端机的位置需要变动时，只需将其插入新地点的插座上，然后做一些简单的跳线即可，不需要再布放新的线缆，也不需要再安装新的插孔。另外，SCS 采用星型结构，系统的管理维护及故障的检查和排除也非常方便。SCS 以其高度的灵活性及多元化服务越来越受到人们的重视。

SCS 可以划分为以下 6 个子系统。

- 工作区子系统(用户端子)。
- 水平布线子系统。
- 干线子系统。
- 设备间子系统。

- 管理子系统。
- 建筑群子系统。

1) 工作区子系统

工作区子系统是结构化综合布线系统中将用户的终端设备连接到布线系统的子系统。工作区子系统所包含的硬件包括信息插座、插座盒(或面板)、连接软线以及适配器或连接器等连接附件。

工作区是一个独立的需要设置终端设备的区域，它的服务面积一般按 5～10 m^2 估算，每个工作区设置一个电话插座和一个计算机插座。信息插座是终端设备与水平子系统连接的接口，8 针模块化信息插座是为所有的综合布线系统推荐的标准 I/O 插座。

信息插座的数量一般由使用者的数量决定，如果使用者的数量不能确定，有一些经验值可供参考。根据经验，在办公环境下一般可考虑 9 m^2 设置一个工作区，安装一对信息插座(一个接电话，一个接计算机)。但这仅是一个参考，在具体设计和施工过程中，设计单位和用户单位应根据具体情况灵活掌握。

2) 水平布线子系统

水平布线子系统是结构化综合布线系统中连接用户工作区与布线系统主干的子系统。水平布线子系统由每层配线间至信息插座的配线电缆和工作区用的信息插座等组成。在结构化综合布线系统中，水平布线子系统起着支线的作用，它将所有用户端通过一些连接件连接到配线设备上。

水平布线方式受到很多因素的影响，常用的布线方式大致有两种：一种是直接铺设管线方式，它采用星状结构，利用金属线槽或金属管从布线系统的干线接线间或卫星接线间直接引到每个信息点；另一种是线槽管道布线法，通常是在天花板内安装线槽，再用管线从线槽引到每个插座。

在新建建筑中，布线系统的设计应在设计大楼的图纸时考虑，并融进大楼的弱电图中，以便在施工过程中暗铺相关的线槽和管线，预留墙面出口，安装插座底盒。

3) 干线子系统

干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。干线子系统是综合布线系统的骨干，包括以下几个方面。

- 供干线电缆走线用的垂直或水平通道。
- 设备间与网络接口之间的连接电缆。
- 设备间与建筑群子系统之间的连接电缆。
- 干线接线间与各卫星接线间之间的连接电缆。
- 主设备间与计算机中心之间的电缆。

综合布线系统的干线可根据距离的远近和用户对传输速率及传输质量的要求，选择大对数双绞线或光缆。一般在楼内的语音通信采用 3 类的大对数双绞线作为主干；数据通信可以采用高品质的 5 类双绞线，也可以采用光缆；如果电磁干扰严重，则推荐采用光缆作为数据主干。在做干线子系统的设计时，首先要确定每一层楼的干线需求，总结出整座楼的干线总体需求，确定干线电缆的种类及其大小尺寸，然后确定干线电缆的路由通道。

干线的路由通道有两大类，即封闭型和开放型。开放型通道通常是指在建筑物的地址集中安装大型通信设备的场所，如 PABX(自动用户小交换机)、大型计算机、计算机网络通

信中枢等。

4) 设备间子系统

设备间子系统主要用来安放网络关键设备，地位十分重要。并非每一个综合布线系统都有设备间子系统，但在大型建筑物中一般是有的，而且有时还不止一个。设备间子系统中的电话、数据、计算机主机设备及其保安配线设备宜设在一个房内。必要时，也可以分别设置，但程控交换机及计算机主机房距离设备间不宜太远。设备间的位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。在设备间子系统的设计和安装过程中，还需要综合考虑配电系统(不间断电源 UPS)和安全因素(设备接地等)。

5) 管理子系统

管理子系统是结构化综合布线系统中对布线电缆进行端接及配线管理的子系统。

管理子系统通常设置在一幢大楼的中央设备机房和各个楼层的配线间，一般由配线架和相应的跳线组成。通过管理子系统，用户可以在配线架上灵活地更改、增加、转换和扩展线路，而不需要专门的工具或专业的技术人员。正是通过这些功能，结构化综合布线系统才具有传统布线无法比拟的开放性、扩展性和灵活性。

6) 建筑群子系统

建筑群子系统是结构化综合布线系统中由连接楼群之间的通信传输介质及各种支持设备组成的子系统。建筑群子系统也称为户外子系统，其传输介质除了各种有线手段之外，还包含其他无线通信手段，如微波、无线电通信等。

户外电缆在进入大楼时通常在入口处经过一次转接接入户内系统，在转接处可以加上电器保护设备。现代化电话通信系统中的通信线路在进入楼群时一般都考虑这一点，主要是避免因雷击或与高压线接触而给人和设备带来的损失。建筑群子系统的布线方式有以下几种：地下管道敷设方式、直埋沟内敷设方式和架空等。不同方式各有其优缺点。

结构化综合布线方面的标准有 EIA/TIA 568A 和 EN 50173，分别是北美和欧洲标准。它们都规定利用铜介质双绞线的特性实现数据链路的平衡传输，只是在抗电磁干扰要求方面有差异。ISO/IEC 11801 是 1995 年由 ISO 确定的国际标准。我国相关规范如下。

- GB/T 50311—2000《建筑与建筑群综合布线系统工程设计规范》。
- GB/T 50312—2000《建筑与建筑群综合布线系统工程验收规范》。
- GB 2887—89《计算站场地技术条件》。
- GB 50174—93《电子计算机机房设计规范》。
- GB 9361—88《计算站场地安全要求》。

3. 网络主干设备安装调试

在网络布线工程完工且验收合格后，一旦选配的局域网主干设备到货，就进入了网络主干构建阶段。构建从设备安装调试开始，通常由设备供应商派出的技术人员进行。网络管理员的任务是在参加设备安装调试工作的同时尽快熟悉系统构建的操作，并且把好安装调试质量关。

网络主干交换设备安装调试的步骤通常如下。

1) 拆箱检验

网络管理员与设备供应商共同打开硬件设备的包装箱，确认其中的设备符合订购要求，确认包装中的内容与装箱单一致，确认设备在运输过程中没有受损，确认所配置的软件、

说明书和附件齐备。

2)　设备安装

网络主干使用的交换机通常都是机架式设备，配备带有风扇的专门机柜。将交换机通过支架安装固定在机柜内。注意：要确认电源插座的电压和设备卡上规定的电压相符，连接好设备电源。

3)　连接网络线缆

交换机上常见的双绞线通信端口有两种：一种是供直接连接用户设备的直通电缆端口；另一种是供与其他交换机连接的级联端口。线缆用的都是 RJ-45 插头，安装时要注意看说明书。

配备千兆以太网的光纤接口交换机，需要使用不同的千兆以太网接口转换器(GBIC)，分别提供对 100Base-LX、1000Base-SX 和 1000Base-LH 等单模光纤和多模光纤使用长波/短波激光信号传输的支持。GBIC 使用 SC(方型接口)类型的光缆插头，光缆另一端使用的插头类型要与所连接的设备匹配。注意：使用光纤跳线时，光纤类型要与 GBIC 支持的光纤类型匹配。最后根据网络设计方案将交换机网络线缆连接好。

4)　连接交换机控制台设备

交换机通常都提供一个串行接口，网络管理员可以通过该接口连接计算机终端设备，监控、配置、调试和管理交换机。通常，技术人员通过交换机配件中提供的转换线缆，将一台笔记本电脑或台式计算机连接到交换机上标识为控制台的串行口，在用作控制台的计算机上启动终端仿真程序。这种管理方式的优点在于无论交换机是否与网络连通，都可以通过计算机进行配置管理操作。

5)　加电调试

在上述准备工作完成后，可以打开交换机电源开关，观察加电自检。通常加电后交换机所有端口的指示灯都闪亮，然后按照设备内置的程序进行硬件检测。在检测时各种指示灯会不断地变化状态，报告检测的进展情况。同时在控制台计算机屏幕上有文字显示。设备加电自检后显示的具体内容随设备的不同而各异，需要仔细阅读说明书。如果一切与说明书所示的情况一样，则表示加电自检通过。

6)　主干设备参数配置

在完成了局域网主干设备的安装调试，设备自检正常，网络线缆连接完毕后，就进入了网络主干设备参数配置阶段。对于一个仅用于小型办公室环境的简单局域网来说，如果数据通信仅限于第 2 层交换，接入层交换机又没有需要上连的主干交换机，设备提供的默认参数往往就可以满足联网要求，将入网设备连接到交换机的端口后，局域网就可以立即开始工作了。

但是，对于一个具有多个层次且结构复杂的局域网而言，必须在完成对所有构成网络主干的交换机的系统参数配置后，局域网才能够正常工作。

通常在进行网络主干设备配置前，应该制订一个计划，并且将计划以文档形式确认下来，画出网络布局示意图。在计划中，应该对各个设备的名称、访问密码、设备地址、设备模块和网络接口配置、设备链路的使用、设备上运行的网络协议和网络管理工作站等做出规定。

进行交换机的参数配置通常有两种途径：通过与交换机控制台端口连接的计算机作为

本地控制台进行配置和通过网络登录作为远程控制台进行配置。

4. 实施注意事项

在网络实施任务中的注意事项如下。

- 选择资质合格的施工单位。
- 加强工程协调。
- 照顾后续施工步骤。
- 把好产品关。
- 把好工程质量关。
- 特别关注光纤布线。
- 注意布线系统的防火。
- 重视屏蔽布线系统的接地问题。

在布线实施的过程中，施工部门必须对所安装的线缆系统进行相关标准的测试，以保证质量的可靠性。

1.3.1.2 测试

测试工作伴随着整个网络工程的全过程，无论是布线安装还是系统调试，都需要进行反复的测试和确定。

1. 测试计划

测试计划应包括下列 5 个方面的内容。

1) 简要说明

简要说明包括工程的概况和需要达到的主要指标。

2) 测试内容

测试内容包括逐项列出的测试步骤、名称、内容和预期达到的目标。

3) 测试清单

测试清单是对每项测试内容列出测试的部位和参与测试的单位，包括进度的安排、测试工具和相应的条件(设备和软件等)。

4) 测试设计说明

测试设计说明是对每项测试内容的测试设计进行考虑，包括测试的控制方式、输入条件和预期的输出结果。

5) 评价准则

评价准则用来说明测试所能检查的范围及其局限性，以及用来判断测试工作是否通过的评价尺度，包括合理的输出结果、测试输出结果与预期输出结果之间容许出现的偏差范围。

测试工作完成后，应提交一份测试分析报告。该报告主要包括下列内容：概要说明、测试结果、结论、原因分析、建议和评价。

2. 网络测试

网络测试是对网络设备、网络系统以及网络对应用的支持进行检测，以展示和证明网络系统能否满足用户在性能、安全性、易用性、可管理性等方面需求的测试。网络测试的实施一般包括以下环节。

- 根据测试目的，确定测试目标。
- 在对相关网络技术和实现细节透彻掌握的基础上，设计测试方案。
- 建立网络负载模型。
- 配置测试环境，包括测试工具的选择及必要的测试工具的研发。
- 采集和整理数据。
- 分析和解释数据。
- 准确、直观、形象地表示测试结果。

网络测试包括网络设备测试、网络系统测试和网络应用测试 3 个层次。

1)　网络设备测试

网络设备测试主要包括以下几个方面：功能测试、可靠性和稳定性测试、一致性测试、互操作性测试和性能测试等。

(1)　功能测试用来验证产品是否具有设计的每一项功能。

(2)　可靠性和稳定性测试往往通过加重负载的办法来分析和评估系统的可靠性和稳定性。

(3)　一致性测试用来验证产品的各项功能是否符合标准。

(4)　互操作性测试用来考查一个网络产品是否能在不同厂家的多种网络产品互联的网络环境中很好地工作。网络产品不同于其他产品的最大特点是必须符合标准，不同的网络产品之间要能互操作。

(5)　性能测试的主要目标是分析产品在各种不同的配置和负载条件下的容量和对负载的处理能力，如交换机的吞吐量、转发延迟等。

典型的网络设备性能测试方法有两种：第一种是将设备放在一个仿真的网络环境中进行测试，第二种是使用专用的网络测试设备对产品进行测试。

2)　网络系统测试和网络应用测试

网络系统测试除了普通意义上的物理连通性、基本功能和一致性的测试以外，主要包括网络系统的规划验证测试、网络系统的性能测试、网络系统的可靠性与可用性的测试与评估、网络流量的测量和模型化等。

(1)　网络系统的规划验证测试主要采用的两个基本手段是模拟和仿真。

- 模拟是通过软件的办法，建立网络系统的模型，模拟实际网络的运行。通过设定各种配置和参数模拟系统的行为，对系统的容量、性能以及对应用的支撑程度给出定量的评价。这对于大型网络的规划设计是不可缺少的环节。
- 仿真是指通过建立典型的试验环境，仿真实际的网络系统。规划验证测试的目的在于分析所采用的网络技术的可行性和合理性，网络设计方案的合理性，所选网络设备的功能、性能等是否能够合理地、有效地支持网络系统的设计目标。

(2)　网络系统的性能测试是指通过对网络系统的被动测量和主动测量来确定系统中站点的可达性、网络系统的吞吐量、传输速率、带宽利用率、丢包率、服务器和网络设备的响应时间、产生最大网络流量的应用和用户，以及服务质量等。此项工作同时可以发现系统的物理连接和系统配置中的问题，确定网络瓶颈，发现网络问题。测试设备记录一段时间内的网络流量，实时和非实时地分析数据。被动测量不干涉网络的正常工作，不影响网络的性能。主动测量向网络发送特定类型的数据包或网络应用，以便分析系统的行为。

(3) 网络系统的可靠性与可用性的测试与评估。系统可用性取决于系统的可靠性(MTTF)及可维护性(MTTR)的高低，其中可靠性是指系统服务多久不中断，可维护性是指服务中断后多久可恢复。三者之间满足如下关系：

$$\text{System Usability} = \text{MTTF} / (\text{MTTF} + \text{MTTR}) * 100\%$$

其中，MTTF 是指平均无故障时间，MTTR 是指平均故障修复时间，MTBF 是指平均故障间隔时间。有 MTBF = MTTF + MTTR，故

$$\text{System Usability} = \text{MTTF} / \text{MTBR} * 100\%$$

(4) 网络流量的测量和模型化。网络流量的测量和模型化对于分析网络性能和带宽的利用率、指导网络流量管理、开发高效的网络应用十分重要。这方面的工作主要有以下几个方面。

- 产生已知特征的流量，使该流量沿网络传播，最后回到测试仪。记录和分析流量特性的任何改变(如延迟漂移)。
- 对链路总体流量的测量和传输时间、吞吐量、带宽利用率等进行分析。
- 分析特定流量的特征和提供的 QoS；收集一个时间段内的测量数据进行分析，分析流量沿网络传播过程中流量特征的变化和网络流量的统计行为，建立流量模型。

(5) 网络应用层次上的测试则主要体现在测试网络对应用的支持水平，如网络应用的性能和服务质量的测试等。例如，部署基于 IP 的语音传输 VoIP 时，最直接的问题是网络中的交换机和路由器设备能否有效地支持语音传输，网络能支持多大的语音流量、多少个语音通道；如果网络支持 VoIP，对网络的其他业务特别是关键业务，会产生什么样的影响；网络是否支持服务质量 QoS。这些问题都需要通过网络应用测试来回答。

(6) 网络系统测试的核心工具是协议分析仪。这是一种专用的网络测试设备，它能够连接到网络上，产生并向网络发送数据，捕捉网络数据，分析数据。协议分析仪一般具有网络监测、故障查找、协议解码和流量产生等功能。

3. 网络设备安全性测试

现在有很多新型网络设备尤其是网络边缘路由器增加了防护功能，阻止了人为、故意的网络攻击。然而，提供的防护会不会对正常数据转发造成影响？有什么样的影响？这些很难从理论上估计，需要进行必要的网络设备安全性测试。

本节提到的测试项，主要是验证网络设备所提供的基本安全功能，并检测这些安全功能项对网络设备运行造成的影响。这些测试项分为访问列表测试和 DOS 攻击测试两大类。

1) 访问列表测试

访问列表测试用于检测边缘路由器的访问列表能否起到防火墙的作用，访问列表测试控制网络传输过滤数据报文，访问列表测试阻止或允许数据报文通过网络接口。过滤依据可以是源地址、目的地址和上层协议号。边缘路由器通过将进入或离开的数据报文与访问列表中的过滤项进行比较，决定允许或阻止数据报文通过。对于边缘路由器能提供的访问列表容量，以及不断变化的访问列表对数据转发的影响都要进行测试。

2) DOS 攻击测试

DOS 攻击测试用于检测边缘路由设备抵抗“拒绝服务(DOS)攻击”的能力。当设备由于伪造的服务请求和虚假的传输而变得非常繁忙时，就无法响应正常的服务请求，从而造成

损失。DOS 攻击测试考验网络设备检测并阻止某种特定攻击的能力，并在检测受到某种攻击、设备超负荷运行的情况下，正常传输转发性能所受的影响。

具体的网络设备安全性测试项目如下。

- 访问列表性能测试。
- 虚假源地址攻击测试。
- LAND 攻击检查。
- SYN 风暴检查。
- Smurf 攻击检查。
- Ping 风暴检查。
- Teardrop 攻击检查。
- Ping to Death 检查。

4. 性能测试

性能测试包括可靠性测试、功能/特性测试、吞吐量测试、衰减测试、容量规划测试、响应时间测试、可接受性测试和网络瓶颈测试等。

1) 可靠性测试

可靠性测试是使被测网络在较长时间内(通常是 24～72 小时)经受较大负载，通过监视网络中发生的错误和出现的故障，验证在高强度环境中网络系统的存活能力，也就是它的可靠性。可靠性测试可作为接受性测试的一部分，在产品评估测试中可作为比较测试或作为产品升级进行的衰减测试的一部分。采用的负载模式很重要，越贴近真实负载模式越好。可靠性测试中使用网络分析仪监控网络运行，捕获网络错误。

通常在较长时间段内和持续负载下，不同网络具有不同级别的存活度。如果测试时间足够长、负载足够大，所有可靠性测试最终都会失败。

可靠性测试应用于网络生命周期中的以下 3 个阶段。

- 计划：作为产品评估测试的一部分，比较不同产品或建立要求规范。
- 开发：验证计划中的要求是否能在系统中完全实现。
- 组建：作为可接受性测试的一部分，在网络运行前进行，核实系统是否达到要求。

2) 功能/特性测试

特性测试核实的是单个命令和应用程序功能，通常用较小的负载完成，关注的是用户界面、应用程序的操作以及用户与计算机之间的互操作。特性测试通常由开发人员在他们的工作台上完成，或是在一个小型网络环境下由测试人员完成。

功能测试是面向网络的，核实的是应用程序的多用户特征和在重负载下后台功能是否能正确地执行，关注的是当多个用户正在运行应用程序时，网络和文件系统或数据库服务器之间的交互。功能测试要求网络的配置和负载非常接近于运行环境下的模式。该测试可以在运行网络或独立网络实验室里完成。它只应用于网络生命周期中的以下 3 个阶段。

- 开发：用于核实在期望的运行模式下，在多用户环境里，应用程序的运行性能是否达到要求。
- 组建：在应用程序安装前完成，可独立进行，也可作为接受性测试的一部分，用于核实在期望的运行模式下，应用程序的运行性能是否达到要求。

- ◆ 运行：该阶段测试是在应用程序运行后进行的，如果在运行系统中遇到了问题，该阶段测试用于核实应用程序是否如最初应用时那样工作。

3) 吞吐量测试

吞吐量测试和应用程序的响应时间测试相似，但检测的是每秒钟传输数据的字节数和数据报文数，而不是响应时间。它用于检测服务器、磁盘子系统、适配卡/驱动连接、网桥、路由器、集线器、交换器和通信连接。吞吐量测试用于测量网络性能、找到网络瓶颈，以及比较不同产品的性能。

吞吐量测试不使用程序脚本，它借助某些软件对网络服务器执行文件输入/输出操作来产生流量，或通过某些软件在网络上发送专门的数据报文或帧。该测试应用于网络生命周期的以下几个阶段。

- ◆ 计划：用于比较网络产品，为模拟网络节点提供运行特征和要求规范。
- ◆ 开发：用于核实网络组件以及整个网络是否达到规范要求的水平。
- ◆ 组建：可独立进行或作为可接受性测试的一部分，在网络组件或整个网络正式运行之前核实它们是否满足规范的要求。

4) 衰减测试

衰减测试是将硬件或软件的新版本与当前版本在性能、可靠性和功能等方面进行比较，同时验证产品升级对网络的性能不会有不良影响。衰减测试混杂了很多为完成其他测试任务要进行的测试。衰减测试的关键是要保证被测组件应是运行网络中最关键或最脆弱的组件。

衰减测试不强调升级版的新特性。新特性测试在衰减测试之前作为功能/特征测试的一部分就已完成。尽管新产品应该解决了当前版本中的错误，但它们也经常存在一些以前没有出现过的错误，如果这些错误发生在产品的关键部分，将会引起严重问题。衰减测试不需要测试产品的所有特性，但网络用户正常运行所依靠的关键功能必须在测试之列。

衰减测试应用于网络生命周期的以下两个阶段。

- ◆ 开发：用于核实产品升级版是否能满足性能、互操作性和可靠性的要求。
- ◆ 升级：在采用升级版本之前用该项测试来比较升级版和当前版，看升级版是否和当前版一样满足性能、互操作性和可靠性的要求。

5) 容量规划测试

容量规划测试用于检测当前网络中是否存在多余的容量空间。当网络承受的总负载超过网络总容量时，网络的性能或吞吐量就有可能下降，所以在网络负载接近这一临界点(网络的最大容量)前，就要根据负载增长的幅度扩充网络资源。

进行该项测试要逐渐增加网络负载，直到网络的运行性能、可接受的水平或吞吐量不断下降，达不到设计所要求的水平为止。网络运行负载和网络最大吞吐量之间的差额就是现有系统的冗余量。

容量规划测试应用于网络生命周期的以下 3 个阶段。

- ◆ 计划：用于估计实施该系统所需要的资源，也可用于成本分析和制定预算。
- ◆ 开发：检测系统要求的资源是否满足特定的响应时间和吞吐量的要求。
- ◆ 升级：当系统响应时间或吞吐量下降时，重新选取网络组件。

6)　响应时间测试

响应时间测试用于检测系统完成一系列任务所需的时间，本项测试是用户最关心的。对于表示层，如微软的 Windows，该测试是指在不同桌面之间切换或装载新负载所需的时间。在不同负载即不同实际或模拟用户的数目下运行这一实验，可对每个被测试的应用程序生成一个负载—响应时间曲线。

在应用程序测试中，可执行一系列典型网络动作的命令，如打开、读、写、查找和关闭文件，这些命令提供了最好的负载模拟。例如，对每个进行测试的工作站，检测它在几秒内能完成这些命令。

响应时间测试应用于网络生命周期的以下几个阶段。

- 计划：使用模拟应用程序进行，检测规范要求的各项网络服务。
- 开发：检验规范要求的网络服务是否正在被实现。
- 组建：在接受和组建之前，核实规范要求下的网络服务是否已经被实现。
- 运行：检测网络服务的基准和变化，这可能是针对系统质量的最好测试。

响应时间测试应该包括对系统可靠性的检测。常见的可靠性问题，如在路由器或服务器中大量丢失数据报文或由于网络组件故障引发大量坏数据报文，将严重影响网络的响应时间，因此在整个测试期间都应用网络分析仪监视系统错误。

7)　可接受性测试

可接受性测试是在系统正式实施前的“试运行”。它是一个非常有效的方法，可确保新系统能提供良好而稳定的性能。和衰减测试一样，可接受性测试中也包含多项测试，如响应时间测试、稳定性测试和功能/特性测试。

可接受性测试应用于许多领域，但在安装或升级网络前应进行的网络可接受性测试则经常被忽略，而事实上，可接受性测试能为网络购买者在经济和技术上提供有力的保证和参考。

可接受性测试可以仅在新增加的部件上完成，将已存在的负载加上新增程序或新增组件可能产生的负载作为测试使用的负载。

可接受性测试应用于网络生命周期的以下两个阶段。

- 开发：在开发阶段前定期执行，用来核实要求的标准是否可行。
- 组建：在网络投入运行之前应用，用来核实系统是否满足所有要求。

8)　网络瓶颈测试

通过网络瓶颈测试可以找到导致系统性能下降的瓶颈。测试中需要测试和计算系统的最大吞吐量，然后再在单个网络组件上进行该项测试，明确各组件的最大吞吐量。通过计算单个组件的最大吞吐量和系统最大吞吐量之间的差额，就能发现系统瓶颈的位置以及哪些组件有多余的容量。

系统瓶颈在不同的测试案例中出现的位置可能有所变化。例如，一个客户业务应用程序测试可能表明服务器是系统的瓶颈，而对一个电子邮件系统的测试则可能表明广域网连接才是网络的限制因素。如果可以在测试的环境中重现引起问题的负载，那么这样的测试结果对解决问题将有很大帮助。

瓶颈测试应用于网络生命周期的以下两个阶段。

- 组建：可以作为容量计划的一部分，用于帮助相关人员明确影响网络性能和响应时间的瓶颈位置。

- 运行：作为故障检测的一部分，帮助相关人员找出影响网络性能或引起系统问题的网络瓶颈。

5. 测试报告

测试报告是整个项目的第一份供大家交流和供领导查阅的报告，人们对工程的满意程度和对工程质量的认可很大程度上来源于这份报告。通常在独立网络测试后，要总结测试数据，并基于此对测试过的同类产品进行排序；而系统内部的测试仅是得出一个简单的结论。

测试报告呈现的内容和采取的表现形式非常重要，测试报告通常包含以下信息。

- 测试目的：用一句或两句话解释本次测试的目的。
- 结论：从测试中得到的信息推荐下一步的行动。
- 测试结果总结：对测试进行总结并由此得出结论。
- 测试内容和方法：简单地描述测试是怎样进行的，应该包括负载模式、测试脚本和数据收集方法，并且要解释采取的测试方法怎样保证测试结果和测试目的的相关性，以及测试结果是否可重现。
- 测试配置：网络测试配置用图形表示出来。

测试报告的形式可以是一个简短的总结(2～4 页)，也可以是一个很长的书面文档(5～20 页)。测试总结可以使用图形表示测试结果，如应用程序的响应时间、吞吐量和产品评估。而系统衰减性测试、配置规模测试和应用程序的功能/特性测试的测试报告还要包括更多的信息。

在非常特殊的情况下，测试报告需要长达 50 页。它通常包括从项目开始到结束按时间编排的所有活动，以及非常详细的问题信息和解决问题的信息。

6. 网络测试工具

网络测试工具一般包括以下几个。

- 网络管理和监控工具。
- 建模和仿真工具。
- 服务质量和服务级别管理工具。

网络管理和监控工具(如 HP 公司的 OpenView)能够在网络测试运行过程中提示某些问题的网络事件的出现。这些工具可以是驻留在网络设备中的应用软件。

协议分析仪也能被用于监测新设计的网络，帮助分析通信的行为、差错、利用率、效率以及广播和多播分组。

建模工具和仿真工具是更为先进的用来测试验证网络设计的工具。仿真就是在不建立实际网络的情况下，使用软件和数学模型来分析网络行为的过程。利用仿真工具，可以根据所需要测试的目标开发一个网络模型，从而估计网络性能，并对各种网络实现方法之间的差异进行比较。仿真工具使得选择比较的空间变得更大，特别适合于实现和检查一个扩展的原型系统。一个好的仿真工具往往非常昂贵，实现的技术也比较复杂，它要求开发人员不但要精通统计分析和建模技术，而且还要对计算机网络有所了解。

服务级别管理工具是一种比较新型的工具，主要用来分析网络应用的端到端性能。有些工具能够管理服务质量和服务级别，有些工具能够监控实时应用的性能，有些工具能够预测新的应用性能，有些工具可以将上述功能结合起来实现更强大的功能。

1.3.1.3　评估

评估测试不只针对物理设备，更重要的是要评估、比较各种网络技术。通常使用模拟测试配置和模拟负载进行子系统(如路由器)和网络技术(如 ATM 或 FDDI 等)的评估。评估测试不适用于全局网络，因为全局网络拓扑负载、网络设备太多，不好准确定位引起问题的原因和位置，不能进行有效的比较。多数评估测试在专用的子网测试环境中进行。

很多公司都有其固定合作的网络设备供应商，如路由器、集线器或交换机的供应商，通常很少再做设备比较测试，但网络技术的比较测试需要经常进行。企业经常面对选择哪种技术以及怎样比较不同技术的问题，所以技术评估是评估测试中很重要的一项。

在比较设备与技术时，除了使用专用于待测设备或技术的工程负载外，有经验的程序员也使用真实负载，使用真实负载可以了解待测设备或技术在特定环境下的运行性能。通过两种负载模式检测结果的比较，可以获知待测设备还有多少多余容量。

评估测试与设备或技术的功能/特征测试一样，用于比较待测设备或技术的性能、稳定性、特性、易用性配置和管理等方面的功能。

评估测试实质是衰减测试的基础，评估测试中对几种设备或技术进行比较；衰减测试中对同一设备的不同版本进行比较。测试中选择设备的标准也完全可作为验证升级版本工作正常与否的标准。尽可能多地集成在计划/设计阶段进行测试是非常好的方法，最初的产品评估测试可以被开发阶段的可接受性测试和升级阶段的衰减性测试所借鉴。

评估测试是最常进行的测试，在设备选型、技术选型，以及网络系统升级过程中都要进行或多或少的评估测试。

用于评估测试的负载模式和测试脚本要能有效覆盖被检测的设备和技术。常使用最好情形(工程负载)和真实负载模式进行测试，两种方式都提供了唯一的、重要的检测结果，测试人员要能够理解、解释测试结果间的不同。

工程检测结果是被测设备和技术在最理想的情形下测试得到的结果，因此不能在真实运行环境里显示它们的运行性能；真实检测结果能很好地显示待测设备或技术在运行网络环境中的性能，但无法预测设备的总容量。如果时间允许，两种测试都要做。通常测试人员只有时间进行一种测试，一般进行最好情形的测试。许多公开发行的测试报告都是基于最好情形(工程负载)下的测试结果。

所有的测试配置都是模拟的。用于设备比较的测试配置不一定要代表运行网络的典型配置，任何有效、公正的测试配置都能对被测产品进行很好的比较。然而，测试配置和负载越接近运行网络的配置和负载，测试的结果越能反映被测设备在运行网络中的运行情况。

在安装和配置测试网络时必须注意：要确保配置中所有测试组件都是最新版本，使测试尽可能地公正和统一，以取得最好的测试结果。在测试非正式版时一定要小心，因为发布日期经常有错误。测试配置中安装了非正式版后，它还可能会变，所以非正式版的测试结果和正式版的测试结果经常不一致，分析非正式版的设备经常会延误项目的进行。

进行评估测试时，除了被测设备，测试配置中的所有网络组件都要保持不变。这一点非常重要，只有这样才能保证被测设备可以进行公平比较。对于子网，这一点很容易做到(一个网络设备很容易被另一个设备所替代)。

网络技术评估要比较各种网络技术，因而测试配置中的几个网络组件都需要更换。重要的是不要改变源或目标配置。在配置中不仅通信线路需要更换，路由器也需要更换。传

输负载和端点的配置要保持不变。

需要评估测试计划中的各个测试任务，逐步完成测试、数据收集和数据解释。在评估测试中，各测试进行的先后次序没有关系，因为它们不是线性关系，而是多次重复进行的。当在测试中发现了新的信息时，以前所做的测试可能要重新进行以确定它的测试结果，或要对以前的测试稍作改变以检验网络运行的其他方面。此外，在评估期间设备提供商经常发布新的版本或非正式的版本，所以各种基于这种设备的测试都要重新进行。

制定网络设备、技术比较或取舍标准时，不仅要参考评估测试所得的测试结果数据，还要综合考虑其他一些信息，如各设备的性能价格比，但由于没有运行网络的持续和峰值负载要求，所以缺少比较基准，往往将产品评估测试引入歧途。

最后要根据评估测试所得的数据和图表对网络系统作出总结性评估，并撰写网络系统评估报告。

1.3.1.4 转换到新网络的工作计划

转换到新网络是一件复杂的过程，需要仔细筹划，推荐按以下步骤进行。

1. 评估

在转移到新网络以前，首先对系统进行测试，即将本单位的主要软件迁移至新网络上进行运行测试，查看测试结果，并记录下系统是否符合建议书中的要求。要特别注意新用户的登录界面、重要应用软件的运行方式、系统的响应时间、升级带来的新特征。这种方案确保测试是对软件的全面测试。

2. 培训

如果由上一阶段的结果确定新网络是可行的，那么可以全面投入使用。接下来就是制订培训计划，培训在新网络环境中的用户和管理员。

3. 预实施

预实施作为实施迁移的第一步，应该细化迁移计划书中的时间表和计划表，使它成为实施迁移的详细的工程计划。在计划书中，确定需要迁移的用户标识名。查看已存在的服务器，决定哪些设备、文件、目录应该被移植，哪些应被压缩。在迁移到新网络之前，需要提前通知所有用户做好准备。

4. 迁移

选择一个适当的迁移时间，最好定在单位事务不繁忙的时候(如周末)。事先做好系统软件和数据的备份，然后逐步将原有系统安装部署到新网络中，并做好相关设备的配置。要一边安装一边测试，注意不但要用管理员身份测试，还要用普通用户身份测试，以确保迁移后的系统与原有系统一致。

5. 迁移之后

当网络迁移工作完成之后，要开放网络的登录，通知用户新网络开通。要仔细回顾升级过程，以便总结教训，更有效地升级其他服务器，减少遇到的麻烦。要努力理解由升级产生的各种支持要求。应继续测试新的系统，在必要的时候优化系统，争取在对用户造成问题之前就排除它们。

若发现某部分迁移后影响了原有功能，在无法迅速解决问题之前，可以暂时撤销迁移而继续采用原有系统。

1.3.2　典型例题分析

下面哪一种办法可以消除以太网阻塞?

(1)　启用全双工以太网。

(2)　在以太网络中冲突难以彻底避免。

(3)　启用半双工以太网。

(4)　将共享 Hub 全部替换成以太网交换机。

(5)　创建 VLAN。

答案：启用全双工以太网。

解析：消除阻塞的唯一办法是使用全双工以太网。全双工的以太网允许一个工作站同时发送和接收数据。以太网的交换机减少了阻塞的可能性，但是，如果一个设备处于半双工状态，它就有可能存在同时接收和发送的情况，这就可能造成阻塞。

1.3.3　同步练习

1. 第三层交换机的哪些功能可用在接入层?

2. 指出下列各模块中会出现哪些设备(注意：一些设备可能出现在多个模块中)。

模块：电子商务模块、因特网连接模块、远程接入与 VPN 模块。

设备：Web 服务器、SMTP 邮件服务器、防火墙、网络入侵检测系统(NIDS)工具、DNS 服务器、VPN 集中器、公共 FTP 服务器。

1.3.4　同步练习参考答案

1. **答案**：

可用在接入层的第三层交换机的功能如下。

- 广播域(包括 VLAN)之间的路由选择。
- 使用不同的广域网技术访问远程办公室。
- 路由传播。
- 分组过滤。
- 验证与安全性。
- 服务质量(QoS)。
- 按需路由选择(DDK)和静态路由选择。

2. **答案**：

电子商务模块：Web 服务器、防火墙、网络入侵检测系统(NIDS)工具。

因特网连接模块：SMTP 邮件服务器、防火墙、公共 FTP 服务器、DNS 服务器。

远程接入与 VPN 模块：VPN 集中器、网络入侵检测系统(NIDS)工具、防火墙。

1.4 网络系统的运行和维护

1.4.1 考点辅导

1.4.1.1 用户措施

1. 用户管理

用户(User)是网络系统的主要使用者，使用网络的单位和个人都属于用户范畴。用户的身份决定其在网络系统中的权限，不同身份的用户在网络系统中担任着不同的角色(Role)。

在网络中必须有严格的用户管理措施，以保证网络的正常使用和运转。系统管理员是网络系统的维护人员，他的重要任务之一就是管理用户，他本人也是用户，但拥有比其他用户更高的权限。

用户在使用网络系统之前需要注册，即将用户信息提交给网络管理员审阅，通过后即可开通服务。用户在使用网络资源的过程中必须接受管理员的管理和网络管理程序的控制，用户的行为必须遵守既定网络管理规则。

网络用户管理包括以下内容。

(1) 局域网用户管理：局域网用户的创建、注销和访问权限管理，主域用户资料数据库的维护和管理。

(2) 电子邮件用户管理：电子邮件用户开户审核，用户创建、注销和权限管理，电子邮件用户数据库的维护。

(3) 用户入网设备 IP 地址管理：局域网用户的 IP 网络地址分配和技术支持，用户 IP 地址分配数据库的维护。

(4) 用户 Internet 访问管理：Internet 访问权限管理、传输内容监控和费用分配控制管理，用户流量数据库管理和维护。

在局域网环境中存在多种网络应用和管理系统，每个系统都含有一套独立的用户身份认证管理系统。为了有效地管理用户信息并利用这些信息提高网络管理效率，需要建立统一的身份认证系统，目前用户信息管理系统大都建立在轻量目录访问协议(Lightweight Directory Access Protocol，LDAP)的基础之上。

2. 用户培训

用户培训是保证系统正常运行的重要因素，需要针对不同层次的用户进行不同内容的培训。用户培训需要经过以下几个过程。

(1) 培训需求。调查哪些用户需要培训。

(2) 需求分析。进一步分析用户的培训需要，总体设计培训流程。

(3) 课程定制。针对不同的用户制订不同的课程计划和授课内容、预期目标等。

(4) 确定师资。选择有经验的教师教授课程，教师必须熟悉课程及相关内容。

(5) 培训实施。确定培训时间段和授课计划。

(6) 信息反馈。及时对培训效果进行调查，以便调整后期培训方案。

用户培训是一个不断完善的过程，每一期的培训经验都应带入到下一次培训中。随着网络系统的升级和大量网络新技术的使用，用户培训需要经常开展，以便用户能够更好地了解和使用网络服务，最大限度地发挥网络效益。

3. 用户协商

用户的要求永远都是网络存在的依据，所以网络系统提供的服务必须随时能够满足用户的需要，应该认真听取用户对于网络系统的服务质量的意见并尽量改进。应该定期征求用户的意见和要求，可以通过问卷或召开会议的方式，征求他们对于系统运行状况及可能的发展方向的意见，作为日后维护和升级的参考依据。

1.4.1.2　制订维护和升级的策略和计划

网络维护是保障网络正常运行的重要方面，主要包括设备保养与维护、故障检测与排除、网络日常检查、网络性能监控及网络升级等。此处只介绍网络升级的知识，其他部分将在第 5 章详细介绍。

1. 确定策略

当网络出现性能下降、技术老化、用户业务规模扩展时，就意味着原有网络不能再满足用户的需要，此时必须进行网络升级。升级前需要确定升级的策略。

升级的步骤如下。

(1) 评估并确定需求。了解网络环境的运行现状，分析升级的原因。

(2) 制定目标。确定升级要实现的目标。

(3) 制定预算。根据升级的目标确定升级需要更换的部件，根据市场价格制定预算。

(4) 制订规划。详细描述升级计划并形成文档。

(5) 测试规划。对升级计划的可行性进行测试，在必要时调整升级计划。

(6) 用户培训。对升级涉及的用户进行培训，让他们熟悉新系统。

(7) 备份与恢复。在升级前对系统文件和数据进行备份，以便在升级失败时恢复系统。

(8) 实施升级。按照升级计划的内容严格执行升级。

(9) 检查实施情况。评估升级是否达到既定目标。

2. 设备的编址

在升级的过程中需要对使用的设备(如服务器、工作站、路由器等)进行编址，即给每个设备分配一个 IP 地址，并详细记录每个 IP 地址所对应的部门、位置、机器编号和 MAC 地址等，存入 IP 地址管理数据库，并规定用户不得任意更改以避免 IP 地址冲突。设备的编址也应遵循一定规则，如可以按照部门、位置或机器的型号等进行编址，具体应由网络管理员根据实际情况确定。另外，每个部门的 IP 地址应留有一定的空余，以备今后添加设备之用。

3. 审查的时间

升级规划的审查时间应在升级实施之前，审查一般需要搭建实验环境进行升级规划的测试，测试对象包括规划中用到的设备、协议和软件等，评估升级后的网络对原有网络性能的影响。获得的测试结果可以帮助修正升级规划，以便对其中不合理的部分进行调整，

从而保证升级后的网络系统能够正常运行。

4. 升级的时间

升级的实施应在通过审查后进行，在升级前，应当预先对系统进行备份，以便在升级失败后能够恢复系统。升级应该按照计划严格执行，每完成一个阶段，就应该检查升级的结果并记录。

升级中常用到如下设备、工具和软件。

◆ 工作站和服务器。
◆ 网络适配卡。
◆ 集线器、路由器和交换机。
◆ 测试设备。
◆ 工作组和终端用户软件应用程序。
◆ 数据交互方法。
◆ 管理和控制应用程序(如 SNMP、DHCP、DNS 和 NIS 等)。

1.4.1.3 系统维护的高可靠性技术

1. 备件

在建设一个网络的同时，必须配备相应的备件。备件方式和备件策略的好坏直接影响着最终备件失效后的维修时间。备件离故障点越近，故障的维修时间就越短，网络的可用性就越高。但是如果备件的库存太多又会增加库存的成本，因此需根据实际情况确定备件的更换率、周转时间、备件成本等因素，以便综合分析、确定备件策略。

2. 维护操作

维护操作失当是人为造成设备失效的主要原因，包括因操作流程的不规范和维护人员维护的不及时等。

3. 服务水平

服务水平是体现设备商综合能力的重要因素，它直接影响着一个网络的可靠运营。对设备的定期巡检、对用户需求的快速响应、对设备问题的快速定位和及时处理、对客户的定期培训和交流等都会间接提高网络的可用性。

4. 改进措施

针对备件、维护、服务等方面的常见改进措施如下。

(1) 优化维护体制，建立快速响应的维护队伍，减少业务中断时间。这包括对设备的维修和对传输介质的维修。

(2) 通过提高维护队伍的分布、技术水平，增加对维护人员的技术、流程培训，从而减少操作事故，减少故障定位时间。

(3) 制定完善的备件策略，减少备件的响应时间。

(4) 采购设备时应考虑设备制造商提供的服务水平。

(5) 增加计划性的维护，以减少潜在故障的发生。

1.4.1.4　维护和升级的实施

1. 外部合同要点

网络维护和升级工作可由专门的网络维护服务公司来承担，它们的工作任务涵盖许多方面，除了制定相应的管理制度、提高计算机使用人员的素质外，还包括下面一些具体的工作。

1)　建立技术档案

建立技术档案并为客户提供一份详细清单，包括应用软件的种类、名称、用途、版本号、开发商、参数设置等，以及网络的种类、拓扑结构、网络参数等。这些资料在维护工作中将起着重要作用。

2)　指导和培训

计算机软件使用指导和培训是指协助用户进行应用软件的安装、调试，并协助解决使用中遇到的问题。指导用户更好地使用各类应用软件，可以避免因使用不当而导致的问题。

3)　日常维护

日常维护是指定期上门为客户进行整个计算机网络的维护，现场监测系统的稳定性及运作状况，以保证整个系统的正常运行。

4)　紧急现场维护

紧急现场维护是指在用户遇到问题时及时上门排除故障。

5)　重大时刻现场待命

重大时刻现场待命是指客户网络需要作重大调整或升级时，应该全程在场，随时待命，配合客户和供应商解决任何可能出现的问题。

2. 内部执行要点

网络管理人员需要完成的网络维护的工作内容如下。

1)　病毒防治

病毒对网络系统危害很大，必须定期查杀，以免传播造成损失。

2)　数据备份

数据备份是对网络操作系统、软件和数据的备份，它的目的是在发生故障时恢复系统。

3)　数据整理

定期整理计算机数据，清除无用的数据，修复错误的数据，维护系统的稳定性。

4)　故障排除

发生故障时应及时发现并排除故障，以免造成更大的损失。

5)　硬件维护

保持硬件清洁，有效保护硬盘、交换机等易损硬件，延长设备寿命。硬件出现故障时应及时维修。

6)　指导培训

指导网络用户熟悉重要的操作规程，提高他们的操作能力。

1.4.1.5　系统容错技术

目前，计算机网络覆盖范围不断扩大，面临的新业务和用户也迅速增加。在网络运行

过程中，随时都可能出现各种意想不到的问题，其中的很多问题可能会造成网络故障甚至导致网络瘫痪，如不及时采取措施，将会给用户带来无法挽回的损失。因此，必须采用系统容错技术来解决。容错是指网络系统在出现错误(如硬件故障或用户误操作)的情况下仍能正常运转。

系统容错技术既可以用硬件来实现，也可以用软件来实现，还可以采取软硬件结合的系统容错方案来保证系统的可靠性。

常见的系统容错方案有 NEC 公司的容错服务器方案、NCR 公司的 Lifekeeper for NT、DIGITAL 公司的 NT Cluster 和 Fulltime 公司的 Octopus 等。下面简要介绍几种具有代表性的系统容错技术。

1. NEC 的容错服务器方案

顺应IA(采用英特尔处理器的服务器)架构市场占有率的激增，以及 Windows 2000 Server 及 Linux 在服务器领域的迅猛发展潮流，NEC 公司通过与美国 Stratus 容错公司多年合作后，于 2001 年推出了业界第一台基于 IA 架构、支持 Microsoft Windows 2000 Server 标准操作系统环境的容错服务器。它代表了 Microsoft Windows 平台上世界最高水平的系统可用性。该系列容错服务器采用 Intel 处理器及其他标准服务器部件，由于容错服务器的体系结构属于部件级冗余设计的体系结构，其结构的可靠度指标要比双机集群(Cluster)系统高得多，可以较低成本实现小型机的可靠性。

NEC 公司的 Express 5800/ft 系列在 Windows 及 Linux 平台上的可靠性达到了 99.999%，代表了同等环境下全球最高的系统可用性。这种实时保护技术的来源是 Stratus 连续处理技术(Continuous Processing Design)，它包括步锁(Lockstep)技术、安全故障(Failsafe)软件和激活服务(Active Service)结构 3 个基础。

2. NCR 公司的 Lifekeeper for NT

NCR 公司是一家有着悠久历史的世界知名计算机厂商，在包括高可用性平台产品、电子商业、NT 企业服务器容错等七大尖端技术领域的全球市场占有率居第一。Lifekeeper for NT 软件是 NCR 公司推出的全球第一套基于 NT 操作系统的集群容错软件。Lifekeeper 系列产品在我国金融、邮电、民航、证券等领域已得到广泛的应用，有力地促进了市场经济的发展。

Lifekeeper 是一套完善的实时容错软件，对硬件、操作系统、应用软件、业务数据均具备强大的容错性能。有些公司也推出了自己的数据热备份软件，但这些软件只是做到了数据级备份，而对应用软件(如 SQL Server、Sybase 等)、系统软件(如 Windows NT)、系统硬件(如硬盘、内存、网卡)的容错却无能为力。一旦主服务器出现故障，正常业务将被迫终止且不能在短时间内恢复。

Lifekeeper 正是为满足这一社会需求而适时推出的容错软件，为关键业务的运行提供了保障。它是一个设计良好的集群容错软件，主要表现在以下几个方面。

- 能在主服务器发生技术故障时全自动地实现用户端应用系统以及服务器系统的热切换，真正实现用户端的应用连续性。
- 对备份服务器的硬件配置无任何特殊要求，用户可充分利用其原有的设备，从而大大节省投资。

- 既可支持共享磁盘阵列方式，又能支持纯软件容错的扩展方式，性能稳定可靠，能够给予客户在投入、连接结构等方面充分的选择余地。
- 能够做到同时支持 SQL Server、Sybase、Informix、Oracle、Notes、Exchange、SAP 等多种应用平台的灾难恢复。
- 对 NT、SQL 等数据库平台、硬件、应用软件的任何故障都能分别实现实时侦测，具备周全的容错切换机制。

系统容错技术的应用已经开始从过去的银行业、证券业、电信业等领域进入基础行业，如制造、能源、物流、交通，以及有着 7×24 小时不间断运营需求的中小商业团体和政府。系统容错技术的未来将会向着更高的可用性、更卓越的可维护性方面发展。

1.4.1.6　存储、备份与数据恢复

1. 网络数据存储

数据存储备份技术和存储管理技术源于 20 世纪 70 年代的终端/主机计算模式，由于数据主要集中在主机上，因此，管理方便的海量存储设备——磁带库是当时必备的存储设备。20 世纪 80 年代以后，由于 PC 技术的发展，尤其是 20 世纪 90 年代客户机/服务器模式的普及，数据的分布式存储加剧了数据存储管理的复杂化。

Internet 使存储技术发生了革命性的变化。这种变化主要表现在三个方面：首先是存储容量的急剧膨胀；其次是数据就绪时间的延长(网络数据必须保证全天候处于就绪状态)；最后是数据存储结构发生了巨大变化。在 Internet 和全球化电子商务的时代，数据应该是面向全世界的，数据的存取只应受到安全机制的限制，而不应受到地域空间的约束。

网络环境中破坏数据的因素主要有以下几个方面。

- 自然灾害(如水灾、火灾、雷击、地震等)造成计算机系统的破坏，导致存储数据被破坏或完全丢失。
- 系统管理员及维护人员的误操作。
- 计算机设备故障，其中包括存储介质的老化、失效。
- 病毒感染造成的数据破坏。
- Internet 上“黑客”的侵入和来自内部网的蓄意破坏。

计算机系统不是永远可靠的，双机热备份、磁盘阵列、磁盘镜像、数据库软件的自动复制等功能均不能称为完整的数据存储备份系统，它们解决的只是系统可用性的问题，而网络系统的可靠性问题需要完整的数据存储管理系统来解决。所以说，网络设计方案中如果没有相应的数据存储备份解决方案，就不算是完整的网络系统方案。

目前市场上的存储产品主要有磁盘阵列、磁带库与磁带机、光盘库等，其中磁带设备以其技术成熟、价格低廉、产品齐全、使用方便等优点占据了存储市场的重要地位。

1) 磁盘阵列

磁盘阵列又称为廉价磁盘冗余阵列(Redundant Array of Inexpensive Disks，RAID)，是指将多个类型、容量、接口一致的专用硬盘连成一个阵列，使其能以某种快速、准确和安全的方式读写数据，从而提高数据的存取速度和安全性。因此，磁盘阵列读写方式的基本要求是，在尽可能提高磁盘数据读写速度的前提下，必须确保在一张或多张磁盘失效时，阵列能够有效地防止数据丢失。磁盘阵列的最大特点是数据存取速度快，并将数据有选择性

地分布在多个磁盘上，从而提高系统的数据吞吐率。另外，磁盘阵列还能够免除单块硬盘故障所带来的灾难后果，通过把多个较小容量的硬盘连在智能控制器上，可增加系统的存储容量。因此，磁盘阵列是一种高效、快速、易用的网络存储备份设备。

2) 磁带库与磁带机

磁带库产品包括自动加载磁带机和磁带库，它们实际上是将磁带和磁带机有机结合组成的。

自动加载磁带机是一个位于单机中的磁带驱动器和自动磁带更换装置，它可以从装有多盘磁带的磁带匣中拾取磁带并放入驱动器中，或执行相反的过程。它可以备份 100～200 GB 或者更多的数据。自动加载磁带机能够支持例行备份过程，自动为每日的备份工作装载新的磁带。

磁带库是与自动加载磁带机类似的基于磁带的备份系统，它能够提供基本相似的自动备份和数据恢复功能，但同时具有更先进的技术特点。它的存储容量可达到数百帕字节(PB，1 PB=2^{50} B=1024^5 B=1024^2 GB，约等于一千万亿字节)，可以实现连续备份、自动搜索磁带，也可以在驱动管理软件控制下实现智能恢复、实时监控和统计，使整个数据存储备份过程无须人工干涉。磁带库不仅数据存储量较大，而且在备份效率和人工占用方面拥有无可匹敌的优势。在网络系统中，磁带库通过存储局域网络(Storage Area Network，SAN)系统可形成网络存储系统，提供远程数据访问、数据存储备份，或通过磁带镜像技术实现多磁带库备份，为企业存储提供有力的保障。因此，磁带库无疑是数据仓库、ERP 等大型网络应用的良好存储设备。

3) 光盘塔、光盘库和光盘网络镜像服务器

光盘塔由几台或十几台 CD-ROM 驱动器并联构成，可通过软件来控制某台光驱的读写操作。光盘塔可以同时支持几十个到几百个用户的访问信息。

光盘库实际上是一种可存放几十张或几百张光盘并带有机械臂和一个光盘驱动器的光盘柜。它的库容量极大，机柜中可放几十片甚至上百片光盘片，这种有巨大联机容量的设备非常适用于图书馆一类的信息检索中心，尤其是交互式光盘系统、数字化图书馆系统、实时资料档案中心系统、卡拉 OK 自动点播系统等。光盘库的特点是：安装简单、使用方便，并支持几乎所有的常见网络操作系统及各种常用通信协议，维护、更换与管理非常容易，同时具有较低的成本和价格。又因光盘库普遍内置有高性能处理器、高速缓存器、快速闪存、动态存取内存、网络控制器等智能部件，使得其信息处理能力更强。

光盘网络镜像服务器是继第一代的光盘库和第二代的光盘塔之后，最新开发出的一种可在网络上实现光盘信息共享的网络存储设备。光盘网络镜像服务器不仅具有大型光盘库的超大存储容量，而且还具有与硬盘相同的访问速度，其单位存储成本(分摊到每张光盘上的设备成本)大大低于光盘库和光盘塔。因此光盘网络镜像服务器已开始取代光盘库和光盘塔，逐渐成为光盘网络共享设备中的主流产品。

在网络海量存储备份系统中，磁盘阵列、磁带库和光盘库等存储设备因其信息存储特点的不同，应用环境也有较大的区别。磁盘阵列主要用于网络系统中海量数据的即时存取；磁带库更多的是用于网络系统中海量数据的定期备份；而光盘库则主要用于网络系统中海量数据的访问。

2. 网络备份

网络备份的最终目的是保障网络系统的顺利运行，所以一份优秀的网络备份方案应能够备份系统的所有数据，在网络出现故障甚至损坏时，能够迅速地恢复网络系统和数据，将系统损失降到最低。

为了在整个网络系统内实现全自动的数据存储管理，必须安装网络数据存储管理系统，它能将备份服务器、备份管理软件与智能存储设备等有机地结合。另外，备份系统必须适应系统容量不断增加的要求，并且必须能够支持多平台系统和远程备份操作。

网络数据存储管理系统是指在分布式网络环境下，通过专业的数据存储管理软件，结合相应的硬件和存储设备，来对整个网络的数据备份进行集中管理，从而实现自动化的备份、文件归档、数据分级存储以及灾难恢复等。

网络数据存储管理系统的工作原理是在网络上选择一台应用服务器(当然也可以在网络中另配一台服务器作为专用的备份服务器)作为网络数据存储管理服务器，安装网络数据存储管理服务器端软件，作为整个网络的备份服务器。在备份服务器上连接一台大容量存储设备(磁带机或磁带库)。在网络中其他需要进行数据备份管理的服务器上安装备份客户端软件，通过局域网将数据集中备份到与备份服务器连接的存储设备上。

网络数据存储管理系统的核心是备份管理软件，通过备份软件的计划功能，可为整个企业建立一个完善的备份计划及策略，并可借助备份时的呼叫功能，让所有的服务器备份都能在同一时间进行。备份软件也提供完善的灾难恢复手段，能够将备份硬件的优良特性完全发挥出来，使备份和灾难恢复时间大大缩短，实现网络数据备份的全自动智能化管理。

数据备份的方式有多种，下面以磁带机为例，简述全备份、增量备份和差分备份的区别和应用。

1)　全备份

全备份(Full Backup)就是对整个系统进行完全备份，包括系统和数据。这种备份方式的最大优点是操作比较简单，当发生数据丢失时，只要用一盘磁带就可以完全恢复系统和数据。然而它也有缺点：首先，在备份数据中有很多重复数据存在，它们占用大量的磁带空间，增加了应用系统的运行成本；其次，备份数据量大，备份时间长，不适用于那些业务繁忙，备份时间有限的场合。

2)　增量备份

增量备份(Incremental Backup)就是每次只对上一次备份后增加的和修改过的数据进行备份。这种备份的优点很明显：没有重复的备份数据，既节省了磁带空间，又缩短了备份时间。它的缺点在于发生灾难时，恢复数据比较麻烦；另外这种备份的可靠性也差。在这种备份方式下，各磁带间相互关联，其中任何一盘磁带出了问题都不能完全恢复系统。

3)　差分备份

差分备份(Differential Backup)就是对上一次全备份之后新增加的和修改过的数据进行备份。它需要与全备份配合使用。例如，管理员先在星期一进行一次系统全备份，然后在接下来的几天里，再将当天所有与星期一不同的数据(新的或经改动的)备份到磁带上。

4)　三种备份方案的比较

由上述介绍可以看出，全备份所需时间最长，但恢复时间最短、操作最方便，当系统

中数据量不大时，采用全备份最可靠。差分备份在避免了另外两种策略的缺陷的同时，又具有了它们的所有优点。首先，它无须每天都做系统完全备份，因此备份所需时间短，并节省磁带空间；其次，它的灾难恢复也很方便，系统管理员只需两盘磁带，即星期一的磁带与发生灾难前一天的磁带，就可以将系统完全恢复。在备份时要根据三种方案各自的特点灵活使用。

3. 灾难恢复

灾难恢复的先决条件是要做好备份策略及恢复计划。日常备份制度描述了每天的备份以什么方式、使用什么备份介质进行，是系统备份方案的具体实施细则。在制定完毕后，应严格按照制度进行日常备份，否则将无法恢复系统。

灾难恢复措施在整个备份制度中占有相当重要的地位，因为它关系到系统、软件与数据在经历灾难后能否迅速恢复如初。全盘恢复一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等时，因此也称为系统恢复。

一个完整的灾难备份及恢复方案包括备份硬件、备份软件、备份制度和灾难恢复计划四个部分。若想做到数据万无一失，还需要根据企业自身情况制定日常备份制度和灾难恢复措施，并由管理人员切实执行备份制度，否则数据安全将是空谈。

1.4.1.7 网络系统的配置管理

配置管理的目的在于维护及优化网络，其功能是对网络的组件进行识别、定义、控制和监视，实现网络的某些特定功能并使网络性能达到最优。网络系统时刻处于变化之中，网络系统本身要随着用户的增减、系统应用项目的变化及设备的维修或更新来及时调整网络的配置，使网络能更有效地工作。

网络配置包括配置节点和集中器数量、分布和互联情况、线路的数量和速率，以及设备的通信模板和端口个数等。配置管理可以视网络的规模和能力随需要而改变，一般包括以下内容。

- ◆ 网络资源的自动发现和图形化表示，以及网络资源的管理信息。
- ◆ 网络资源的对象化管理，被管对象和被管对象组的命名管理、初始化和关闭等。
- ◆ 软件及硬件资源与版本数据的管理。
- ◆ 设备端口状态。
- ◆ IP 地址资源分配与管理、网络 IP 地址与 MAC 地址对应及 IP 地址冲突检测。
- ◆ 子网及主机情况。
- ◆ 设备路由信息，系统中有关路由操作的参数配置。
- ◆ 系统配置信息，更改系统的配置。
- ◆ 配置及资产统计报告。

下面简要介绍设备管理、软件管理和网络配置图。

1. 设备管理

设备管理包括资产管理、设备变化的管理和设备配置管理等。

1) 资产管理

资产管理是指检验和跟踪网络上的软硬件。资产管理的第一步是为网络上的每一个节点列出清单，该清单不仅应包括网络上各种设备的总数，还应该包括每个设备的配置文件、

型号、序列号、在网络上的位置以及技术支持的联络方式等。另外，还应该保留公司所购买的软件的记录、版本号、供应商、技术支持和联络方式等。

资产管理工具的选择应依公司的需求而定，可以购买专用的资产管理软件，它们通常能够自动检测网络上的所有设备并把相关信息保存到数据库中，也可以使用电子表格软件来存储资产数据。另外，应该保证资产管理数据库信息随着网络软件和硬件的变化定期地更新(自动或手动)。

资产管理使网络管理和升级更加容易，简化了网络管理员的工作。

2)　设备变化的管理

作为系统管理员，应该时刻关注在网络正常运行或排障过程中的网络系统的改变，以及在管理和升级过程中的网络问题。设备变化的管理系统帮助将网络元件的移位或改变同网络的不同表现联系起来，简化了描绘基准线和测量网络性能的过程。同资产管理系统一样，变化管理系统也应该保持实时更新。但与资产管理不同的是，变化管理的记录不能由专用程序(能够自动发现网络硬件或软件的程序)生成，而必须由网络管理员提供变化发生的具体情况信息。

3)　设备配置管理

配置管理为所有基于命令的或基于 IOS 的交换机和路由器提供了一种访问配置的简单方法。一旦设备处于被管理状态，其配置文件将自动收集配置信息并存放在资源管理服务器上。通过临近系统的日志消息、检查设备清单的变化、安排轮询等可以做到自动更新配置文件。

配置管理的后台进程能够保证配置文件时刻更新。一旦配置文件生成后，管理员便可以对这些文件执行多种任务。常见的任务如下。

- 运行变化报表：找到配置文件的变化，列出变化细节并指明管理员的责任。
- 调试自动报表：无须时刻监督运行报表，便可以生成历史报表。
- 查询配置文件：按照特征串搜索配置文件或其他文件。
- 比较配置文件：找出两个配置文件的差别。
- 创建定义报表：基于配置文件中的文本串生成报表。

很多厂商的设备都提供了完备的配置管理工具，例如 Cisco 除了提供文件管理功能之外，它的 Resource Manager 软件还提供了 NetConfig 工具。利用这个工具，管理员可以对被管理的设备配置进行实时更改和查询。NetConfig 工具还允许管理员创建自定义的模板，它们是一些命令集，用于改变网络中的一个或多个设备，这些自定义的管理命令可以在路由器或交换机上执行。

2. 软件管理

为了保证系统中各种软件能够正常运行，需要对它们进行必要的管理。软件管理除了包括软件正常的维护外，还应包括软件系统的改变。网络上常见的软件改变如下。

- 补丁：对某一段程序的提高或加深。
- 升级：对已有代码的主要改变。
- 修订：对已有代码的部分改变。

通常所说的补丁是对软件特定部分的提高和加强，它区别于软件的升级和修订，只改

变软件程序的一部分，不改动大部分的代码。补丁经常被用于修复代码中的错误(Bug)，或者稍微地增加软件的功能。补丁不是对整个软件包的替换，相反，它是安装在软件之上的。补丁也不仅仅限于网络操作系统软件，还可能针对其他很多软件。在维护网络的过程中需要管理网络各个不同部分的补丁，有时甚至需要补充服务器的操作系统。

尽管对每种类型的软件的改变不同，但是通常的改变步骤可归纳如下。

(1) 考虑改变(不论是补丁、升级还是修订)是否必要。

(2) 研究改变的目的和它对程序可能产生的影响。

(3) 考虑改变是适用于部分用户还是所有用户，应该集中执行还是逐步执行。

(4) 制定在非工作时间的改变进度(除非它是紧急的)并通知用户。

(5) 备份当前的系统或软件。

(6) 防止用户登录处于变动中的系统或部分系统(例如可以限制登录)。

(7) 执行改变(保证按照升级向导进行并记录修改)。

(8) 在改变之后测试整个系统，完整地测试软件并观察结果。

(9) 如果改变成功，则开放该系统并通知用户；否则应恢复旧版本。

网络管理人员应该根据软件提供商的建议升级和补丁软件，这样可以避免出现不必要的网络故障。

3. 网络配置图

网络配置图是一张网络主要设备的部署结构图，它包括网络系统中所有的主要设备、节点和线路，以及它们之间的连接方式和相对的位置关系。从网络配置图中可以获取许多关于网络系统较重要的信息，如网络的拓扑结构、设备配置、传输能力、冗余度等。网络配置图既便于了解网络配置状况，又有利于网络管理人员的日常维护工作。图 1-10 所示为一张典型的校园网络配置图。

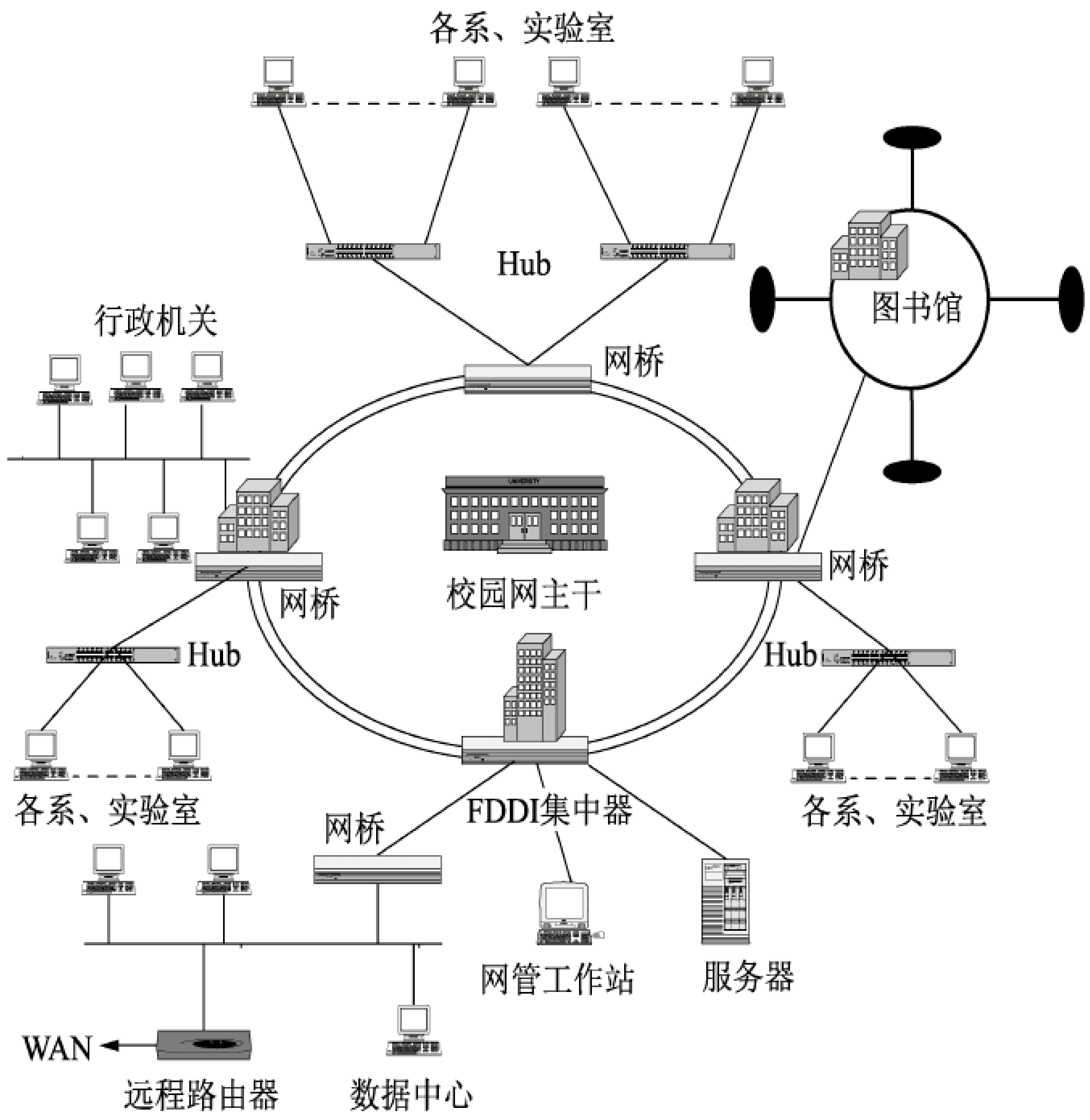


图 1-10　校园网络配置图示例

在配置管理中，通常使用网络配置图将网络的配置用图形表示出来，包括每个组件的名称、IP 地址。对每个网段和广域通信连接，还要标上速率、使用的协议和子网地址。

格式规范的配置文档都应附有网络配置图。

1.4.2　典型例题分析

例 1　Windows 组网中采用什么工具来实现域的创建和管理？在什么情况下需要设置“主域”？

答案：通过 PDC(主域控制器)工具来实现域的创建和管理，该进程运行在 Windows NT Server 上。主域被其他域信任，但主域不信任其他域。当有些部门要单独控制它们拥有的资源，但又要求保持集中身份验证时，需要设置主域。

解析：PDC(主域控制器)是在 Windows NT Server 4.0 域或更早的域中运行 Windows NT Server 并对域登录进行身份验证的计算机，该计算机也用来维护域的目录数据库，PDC 跟踪对域中所有计算机账户所做的更改。它是直接接收这些变化的唯一计算机，每个域只有一个 PDC。

例 2　某公司规模扩大，既要考虑保证目前土建装修的效果不被破坏，又要满足网络扩容和企业工作的实际需求，同时还要保证投资不要过大。请为该公司设计网络升级方案。

答案：经过深入分析和研究对比，建议采用无线局域网(WLAN)组网方案来解决网络扩容的问题。

解析：公司的规模扩大，需要对现有网络进行改造升级，但又不能破坏当前的建筑布局，而传统的网络布线(铺设光纤、双绞线等)都必须挖沟开槽，这样势必破坏该公司土建装修的效果，不满足要求，故必须考虑采用其他组网技术。无线局域网(WLAN)是最佳选择，因为它不需要铺设线缆，只需要安装有限个接入点(AP)就可支持一定范围内的无线接入服务。

在一个典型的 WLAN 环境中，有一些进行数据发送和接收的设备，称为接入点(AP)。通常，一个 AP 能够在 30～100 m 的范围内连接多个无线用户。在同时具有有线和无线网络的情况下，AP 可以通过标准的以太网电缆与传统的有线网络相连，作为无线网络和有线网络的连接点。WLAN 的终端用户可通过无线网卡访问网络。

因此，采用 WLAN 方案可以满足该公司的要求，并将新的 WLAN 与旧有的局域网连接起来。另外，这种方案的投资也较节省。

1.4.3　同步练习

1. 网络升级的原则是什么？
2. 网络升级的要求有哪些？
3. 在 Linux 系统中怎样进行用户管理？
4. 网络存储备份系统的设计目标是什么？
5. 什么是基准线？它在网络的维护过程中有何作用？

1.4.4 同步练习参考答案

1. **答案：**

由于网络升级工作涉及很多因素，因此在制订网络升级计划时必须遵循一些基本的原则，并且要明确网络升级的目的，以免产生偏差。网络升级的原则如下。

- 最大限度地保护已有投资。
- 采用成熟的主流技术。
- 实用性与先进性相结合。
- 综合分析、全面考虑网络升级内容。

2. **答案：**

网络升级的主要目的是提高网络性能，满足网络应用的需求。一般来说，通过网络升级，就能够使网络性能在各方面得到改善。网络的升级要求如下。

- 高速率和稳定性。
- 提高网络的可靠性。
- 增加网络系统的安全性。
- 增强系统的能力。
- 易管理性。
- 无故障升级。

3. **答案：**

Red Hat Linux 是一个多用户系统，当一台计算机被多人使用时，通常需要区分用户，因此每个用户需要一个单独的用户名用于登录。另外，单个用户也可以作为用户组的成员。在 Linux 中，用户管理的方法有多种，包括行命令方式、手工方式和图形界面方式等，每种方法各有其优缺点。

1) 系统管理员

系统管理员是特殊的用户，通常一般用户只运行个人的应用程序，属于系统支持方面的工作，则由系统管理员来负责。系统管理员有一个专用账户即 root，登录时输入：

```
$ login root
Password:******
#
```

以 root 为用户名并输入管理员口令即可登录系统，此时用户身份是管理员。也可以使用替换用户命令 su 登录管理员环境。

2) 用户管理

用户管理中主要包括以下一些操作。

(1) 添加用户。添加用户使用 useradd 命令，该命令的选项较多，如不指定则按默认方式处理。useradd 并不为用户设置口令，必须使用 passwd 命令进行口令设置后，该用户才可以正式使用。

(2) 设置口令。建立一个新用户后必须为其设置口令，设置口令的命令是 passwd，系统管理员可以使用该命令为普通用户设置口令，命令格式如下。

```
passwd [-u] [username]
```

(3) 删除用户。使用 userdel 命令删除用户，命令格式如下。

```
userdel [-r] [username]
```

3) 用户组管理

(1) 添加用户组。使用 groupadd 命令添加用户组，命令格式如下。

```
groupadd [-g gid[-o]] [-r] [-f] [group]
```

(2) 删除用户组。使用 groupdel 命令删除用户组，命令格式如下。

```
groupdel [group]
```

(3) 修改用户组属性。使用 groupmod 命令修改用户组属性，命令格式如下。

```
groupmod [-g gid[-o]] [-n group_name][group]
```

另外，还可以使用 LinuxConf 图形工具管理用户和用户组。

4. **答案：**

理想的网络存储备份系统设计应该提供多层的服务，并应该提供如下功能。

- ◆ 集中式管理。
- ◆ 数据库备份和恢复、全自动备份。
- ◆ 在线式索引。
- ◆ 归档管理。
- ◆ 存储介质管理。
- ◆ 分级存储管理。
- ◆ 系统灾难恢复。
- ◆ 满足系统不断增加的需求。

5. **答案：**

正确维护网络的第一步是标记它当前的状态。只有在分析了网络过去的性能之后，才能预测网络将来的状态。测量和记录网络当前状态的操作称为标定基准线(Base Lining)。基准线参数包括主干网的利用率，每日、每小时登录的用户数，网络上运行的协议数，错误的统计数(如巨型包、冲突、坏的部件，或者是碎包等)，网络设备被使用的频率，以及有关哪个用户占用了最多带宽的信息等。

正确掌握网络的基准线，有利于确定网络正常运行的状态，对快速判断异常情况有很大的帮助。

1.5　网络系统的管理和评价

1.5.1　考点辅导

1.5.1.1　网管系统的功能及构成

1. 网络管理功能

在 OSI 系统管理标准中，将开放系统的管理功能划分为 5 个功能领域，即配置管理、性能管理、故障管理、安全管理和计费管理功能领域。这 5 个功能领域覆盖了网络管理所

需的主要功能，为网络管理系统的功能分析、设计和实现提供了基本概念。

1) 配置管理

配置管理是最基本的网络管理功能，负责监测和控制网络的配置状态。具体地讲，就是在网络建立、扩充、改造以及业务的开展过程中，对网络的拓扑结构、资源配备、使用状态等配置信息进行定义、监测和修改。

2) 性能管理

性能管理用来保证有效地运营网络并提供约定的服务质量。在保证各种业务的服务质量(QoS)的同时，尽量提高网络资源的利用率。性能管理包括性能监测功能、性能分析功能和性能管理控制功能。

3) 故障管理

故障管理的作用是迅速发现和纠正网络故障，动态维护网络的有效性。故障管理的主要功能有报警监测、故障定位、测试、业务恢复以及修复等，同时还有维护故障日志的功能。

4) 安全管理

安全管理的作用是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏。安全管理主要包含风险分析功能，安全服务功能，告警、日志和报告功能以及网络管理系统保护功能。

5) 计费管理

计费管理的作用是正确地计算和收取用户使用网络服务的费用，进行网络资源利用率的统计和网络的成本效益核算。计费管理主要提供费率管理功能和账单管理功能。

2. 网管系统的构成

一个完整的网络管理系统由多个部件组成，主要包括以下几个。

- 网络管理协议。
- 网络管理工作站。
- 被管网络部件。
- 管理信息库(MIB)。

作为管理者(Manager)，一个网络系统中可以有一个(或者几个)网络管理工作站。被管理者称作代理(Agent)，网上具有多个被管网络部件。网络管理协议是管理者和被管理者之间的操作规范，而具体的操作对象则是管理信息的集合——管理信息库(Management Information Base，MIB)。

网络管理系统的基本工作流程如下。

(1) 在被管理部件上预置代理。

(2) 网络管理者使用网络管理协议从代理的 MIB 中取得被管网络部件的管理信息，并存入自己的 MIB。

(3) 管理软件通过对 MIB 的分析处理，达到网络监控的管理目的。

1.5.1.2 网络管理协议

网络管理协议是管理者和被管理者之间共同遵循的规则，他们之间可以通过网络管理协议完成管理信息的交换任务。常用的网络管理协议包括 SNMP、MIB-II 和 RMON 等，它

们都是基于 TCP/IP 协议工作的。

1. SNMP

1) SNMP 概述

SNMP 的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。随后对其改进并加入了符合 Internet 定义的 SMI 和 MIB 体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响很大。SNMP 的体系结构如图 1-11 所示。

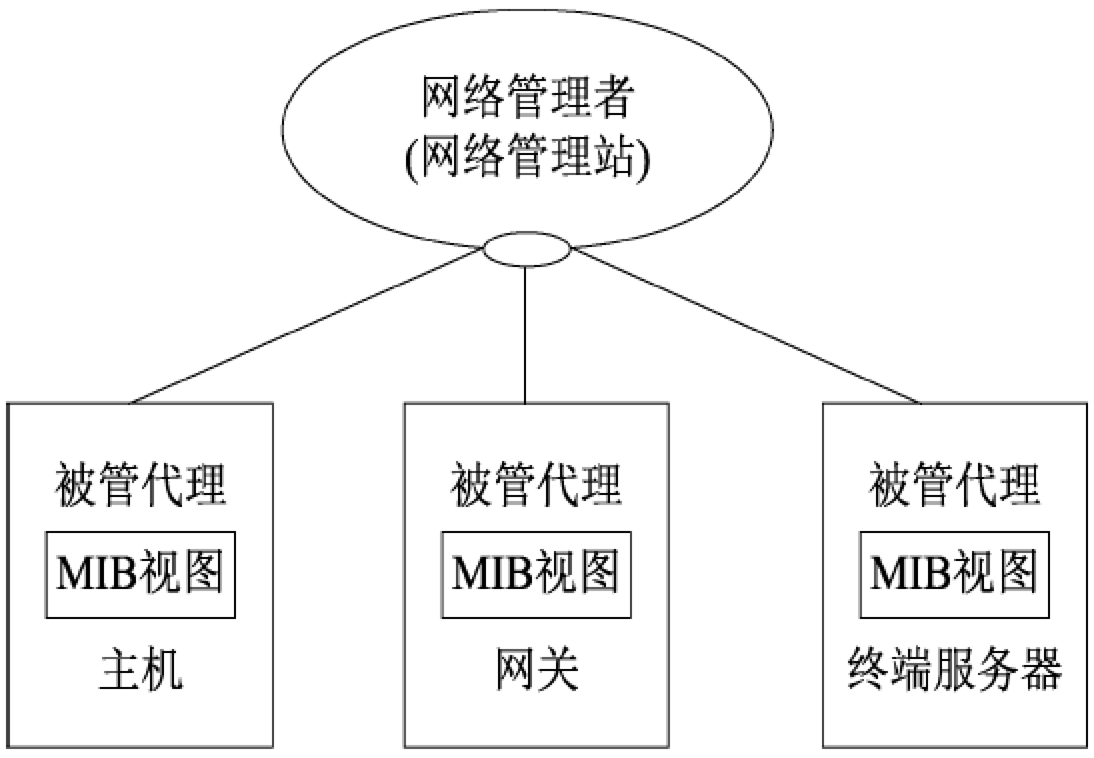


图 1-11 SNMP 的体系结构

SNMP 的体系结构围绕以下 4 个概念和目标进行设计。

- 使管理代理的软件成本尽可能低。
- 最大限度地保持远程管理的功能，以便充分利用 Internet 上的网络资源。
- 体系结构必须有扩充的余地。
- 保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。

在 SNMP 的改进版本 SNMPv2 中，又加入了保证 SNMP 体系本身安全性的目标。

另外，SNMP 中提供了以下 4 类管理操作。

- get 操作：用来提取特定的网络管理信息。
- get-next 操作：通过遍历操作来提供强大的管理信息的提取能力。
- set 操作：用来对管理信息进行控制(修改、设置)。
- trap 操作：用来报告重要的事件。

各种操作的执行如图 1-12 所示。

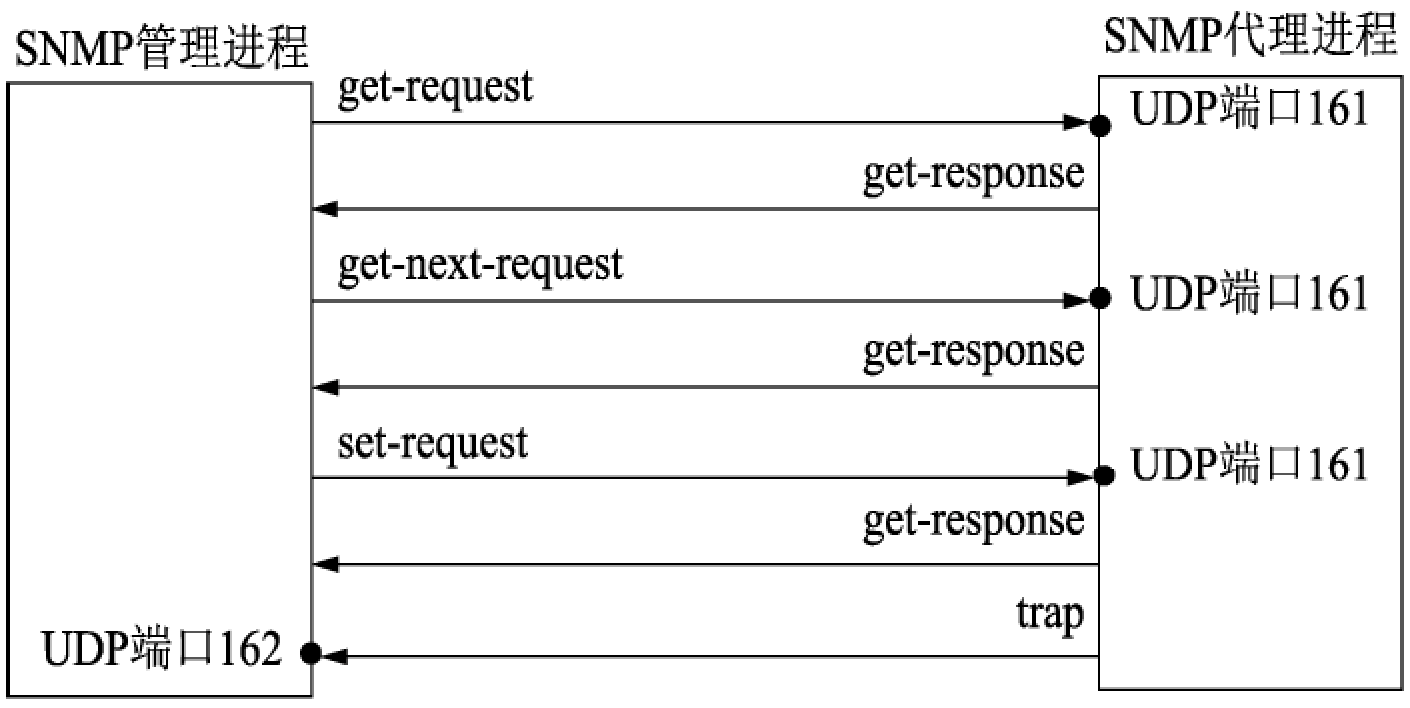


图 1-12 SNMP 的 4 种操作

2) SNMP 管理控制框架与实现

(1) SNMP 管理控制框架。

SNMP 定义了管理进程(Manager)和管理代理(Agent)之间的关系，这个关系被称为共同体(Community)。描述共同体的语义是非常复杂的，但其句法却很简单。位于网络管理工作站(运行管理进程)和各网络元素上，利用 SNMP 相互通信，并对网络进行管理的软件统称为 SNMP 应用实体。若干个应用实体和 SNMP 组合起来形成一个共同体，不同的共同体之间用名字来区分。共同体的名字必须符合 Internet 的层次结构命名规则，由非保留字符串组成。此外，一个 SNMP 应用实体可以加入多个共同体。

SNMP 的应用实体对 Internet 管理信息库中的管理对象进行操作。一个 SNMP 应用实体可操作的管理对象子集称为 SNMP MIB 授权范围。SNMP 应用实体对授权范围内管理对象的访问还有进一步的访问控制限制，比如只读、读/写等；SNMP 体系结构中要求每个共同体都规定其授权范围及其对每个对象的访问方式。记录这些定义的文件被称为共同体定义文件。

SNMP 的报文总是源自每个应用实体，报文中包括该应用实体所在的共同体的名字。这种报文在 SNMP 中称为有身份标识的报文，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用的。管理信息报文中包括以下两部分内容。

- 共同体名：加上发送方的一些标识信息(附加信息)，用以验证发送方确实是共同体中的成员。共同体实际上就是用来实现管理应用实体之间身份鉴别的机制。
- 数据：这是两个管理应用实体之间真正需要交换的信息。

第三版本前的 SNMP 只是实现了简单的身份鉴别，接收方仅凭共同体名来判定收发双方是否在同一个共同体中，而前面提到的附加信息尚未应用。接收方在验明发送报文的管理代理或管理进程的身份后要对其访问权限进行检查。访问权限检查涉及以下因素。

- 一个共同体内各成员可以对哪些对象进行读、写等管理操作，这些可读写对象称为该共同体的授权对象(在授权范围内)。
- 共同体成员对授权范围内每个对象定义了访问模式：只读或可读写。
- 规定授权范围内每个管理对象(类)可进行的操作(包括 get、get-next、set 和 trap)。
- 管理信息库(MIB)限制对每个对象的访问方式 (如 MIB 中可以规定哪些对象只能读而不能写等)。

管理代理通过上述预先定义的访问模式和权限，来决定共同体中其他成员要求的管理对象访问(操作)是否允许。共同体概念同样适用于转换代理(Proxy Agent)，只不过转换代理中包含的对象主要是其他设备的内容。

(2) SNMP 的实现方式。

为了提供遍历管理信息库的手段，SNMP 在其 MIB 中采用了树状命名方法对每个管理对象的实例进行命名。每个对象实例的名字都由对象类名字加上一个后缀构成，对象类的名字是不会相互重复的，因而不同对象类的对象实例之间也很少有重名的危险。

在共同体的定义中一般要规定该共同体授权的管理对象的范围，相应地也就规定了哪些对象实例是该共同体的“管辖范围”。据此，共同体的定义可以想象为一个多叉树，以字典序提供了遍历所有管理对象实例的手段。有了这个手段，SNMP 就可以使用 get-next 操作符，顺序地从一个对象找到下一个对象。get-next(object-instance)操作返回的结果是一

个对象实例的标识符及其相关信息，该对象实例在上面的多叉树中紧排在指定标识符 object-instance 对象的后面。这种手段的优点在于：即使不知道管理对象实例的具体名字，管理系统也能逐个地找到它，并提取到它的有关信息。遍历所有管理对象的过程可以从第一个对象实例开始(这个实例一定要给出)，然后逐次使用 get-next，直到返回一个差错(表示不存在的管理对象实例)结束(完成遍历)。

由于信息是以表格形式(一种数据结构)存放的，在 SNMP 的管理概念中，把所有表格都视为子树，其中一张表格(及其名字)是相应子树的根节点，每个列是根下面的子节点，一列中的每个行则是该列节点下面的子节点，并且是子树的叶节点，如图 1-13 所示。

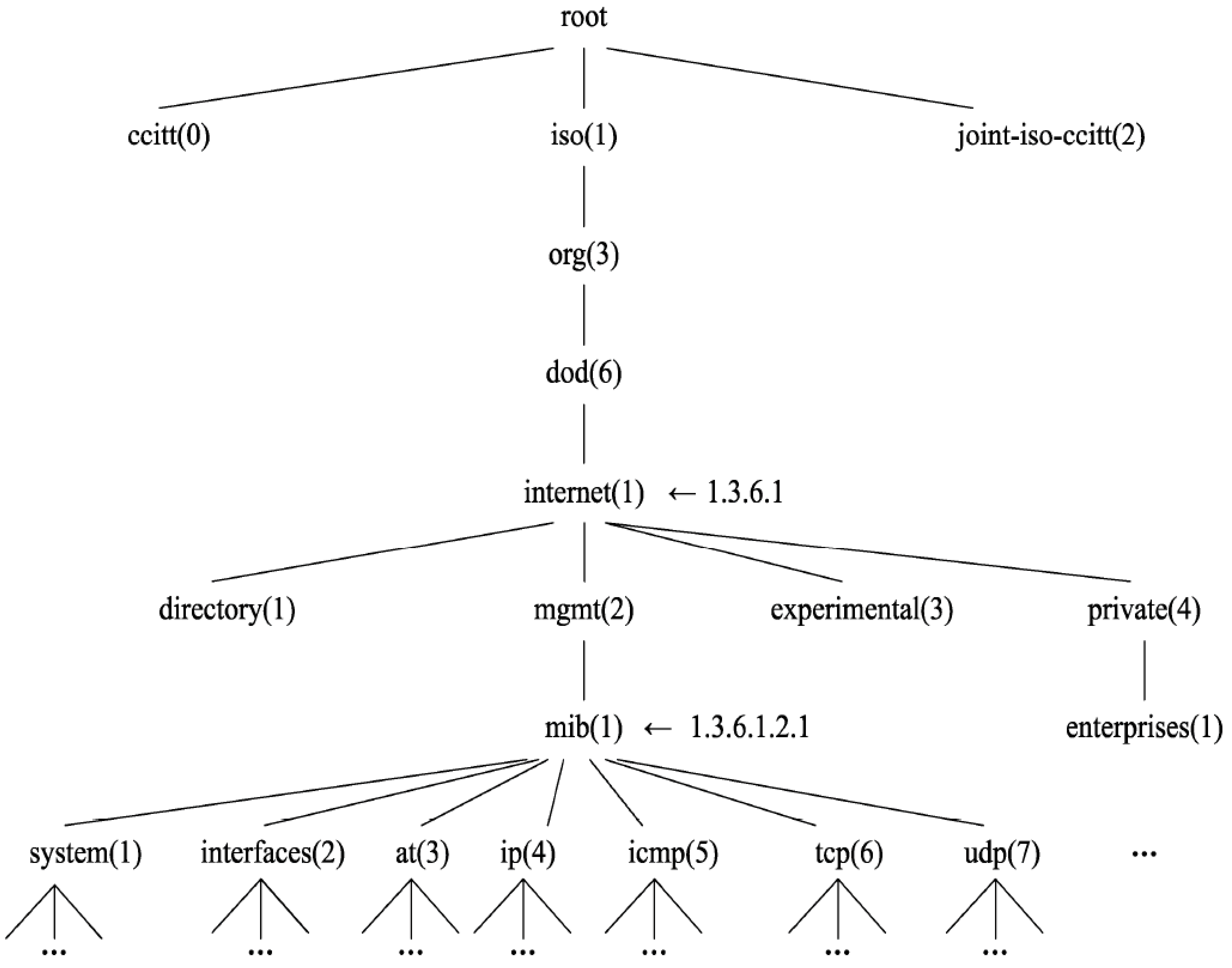


图 1-13　管理信息库中的对象标识

因此，按照前面的子树遍历思路，对表格的遍历是先访问第一列的所有元素，再访问第二列的所有元素……直到最后一个元素。若试图得到最后一个元素的“下一个”元素，则返回差错标记。

SNMP 中的各种管理信息大多以表格形式存在，一个表格对应一个对象类，每个元素对应于该类的一个对象实例。那么，管理信息表对象中单个元素(对象实例)的操作可以用前面提到的 get-next 方法，也可以用 get/set 等操作。下面主要介绍表格内一行信息的整体操作。

- 增加一行：通过 SNMP 只用一次 set 操作就可在一个表格中增加一行。操作中的每个变量都对应于待增加行中的一个列元素，包括对象实例的标识符。
- 删除一行：删除一行也可以通过 SNMP 调用 set 操作，将该行中的任意一个元素(对象实例)设置成“非法”即可。

至于删除一行时，表中的一行元素是否真的在表中消失，则与每个设备(管理代理)的具体实现有关，因此管理进程必须能通过各数据字段的内容来判断数据的合法性。

3) SNMP 协议

SNMP 是一个异步的请求/响应协议，即 SNMP 的请求和响应之间没有必定的时间顺序关系，换句话说，SNMP 是一个面向无连接的协议。这样，SNMP 实体不需要在发出请求后立即等待响应的到来，因此 SNMP 响应也可能丢失或出现错误。

SNMP 中设计了四种基本协议的交互过程。

第一种情况是管理进程从管理代理处提取管理信息。管理进程通过 SNMP 和传输网络发送 get-request 给管理代理，请求中包括管理对象的标识符等参数；管理代理收到请求后返回相应内容的 get-response，响应中包括待提取的管理信息。

第二种情况是管理进程在管理代理的可见范围内遍历一部分管理对象实例。管理进程通过 SNMP 和传输网络发送 get-next-request 给管理代理，管理代理收到后完成遍历的一次操作，用 get-response 将遍历结果返回给管理进程。

第三种情况是管理进程在管理代理中存储信息，即对管理代理的管理信息库(MIB)进行写操作(包括设置工作参数)。管理进程发送一个 set-request 给管理代理，由管理代理完成 set 操作，然后用 set-response 返回操作结果。

第四种情况则是管理代理主动向管理进程报告事件。管理代理通过 SNMP 和传输网络将 trap 发送给管理进程，这个操作没有响应。

注意：上面的各个请求都是管理进程发给管理代理的，响应则都是由管理代理发给管理进程的。只有 trap 是无响应的，由管理代理单向发给管理进程。另外，请求、响应和 trap 的传输处理都要受“共同体”定义的限制，包括访问权限。

SNMP 协议是一个对称协议，没有主从关系。SNMP 上的管理进程和管理代理都可以得到 SNMP 完全相同的服务。下面对 SNMP 协议的部分特点和关键内容进行介绍。

(1) 管理信息报文。

在大多数 SNMP 操作中都使用一个相同的报文数据结构。对于前面提到的身份鉴别方法，报文中包含三种数据(信息)传递给专门的“身份鉴别实体”：共同体名称、有关数据和发送方 SNMP 实体的传输层地址。

身份鉴别实体负责验证发送方是否是合法的对等实体，并返回两种可能的结果：一种结果是返回本次报文中的 SNMP 协议数据类型和发送方 SNMP 实体的权限标识符；另一种结果是返回例外。其中第一种结果表明发送方 SNMP 实体确实是本共同体的成员之一，接收方 SNMP 实体接下来对它进行处理。第二种结果(“例外”)表明发送方 SNMP 实体并非本共同体成员，不能接受此报文，并且接收方 SNMP 实体还可能根据配置产生一个“身份非法”的 trap 事件。

(2) 协议数据单元及其管理操作。

SNMP 协议实体之间的协议数据单元(PDU)只有两种不同的结构和格式，一个 PDU 格式在大部分操作中使用，而另一个则只在 trap 操作中作为 trap 的协议数据单元。

PDU 一般包含多个代表特殊意义的字段：request-id 是一个整数值，用来区分不同的 PDU；error-status 反映管理操作是成功还是失败；error-index 表明操作中哪个变量错误；variable-bindings 是一系列变量的清单，序列中每一项包含一个变量名及其变量值。

在 SNMP 中，接收方完成身份鉴别并得到共同体定义信息之后，SNMP 实体根据 PDU 内容执行以下几种操作：get 操作，根据变量名取出指定的对象实例；get-next 操作，该操

作与 get 操作不同，不是取变量名指定的对象实例，而是取出变量名指定的对象实例的按字典排序的下一个对象实例；set 操作，对指定对象实体的值用请求中的新值替换；get-response 对 get/set 报文做出响应并返回操作结果，收到该响应报文的操作请求方首先根据报文中的 request-id 在记录中查找有无这个序号的请求，如果没有则丢弃该响应，否则接收该响应，管理进程要进行响应处理。

(3)　trap 操作。

trap 是一种捕捉事件并报告的操作，实际上几乎所有网络管理系统和管理协议都具有这种机制。trap 在 OSI 网络管理国际标准中称为“事件和通报”，一般都简称为事件报告。

为了减少管理信息的业务流量，管理代理负责对管理对象的 trap 进行检查，管理检查可以设置检查条件，这样，管理进程就可以在一定程度上控制 trap 报告过程。引入 trap 报告的最大好处是许多重要事件的发生得以及时让管理进程知道。因为一般只有比较关键的 trap 事件才确实需要报告，再加上每个 trap 事件都很简短，因此由于 trap 而引入的不确定管理信息业务量是较少的，但却能大大改善网络管理的时效性。

由于事件多种多样，各种事件的发生环境也不一样，trap 操作的复杂性比前面讲的几种操作都大，SNMP 的 trap 操作 PDU 中的字段类型也较多。这些 trap 操作 PDU 中的字段包括：enterprise，记录发送 trap 事件的管理代理的标识符；agent-addr，管理代理的网络节点地址；generic-trap，描述该 trap 操作报告是哪一种异常事件；specific-trap，给出各管理代理自行定义的 trap 事件代码；time-stam，表示 trap 事件发生的时刻；variable-bindings，给出一组变量，这些变量及其值给出了与 trap 事件有关的详细信息。

当管理代理检测到一个例外或异常事件发生时，管理代理首先要判断需要将该事件报告给哪个或哪些管理进程。对每个管理进程，管理代理要选择相应的共同体号，由 SNMP 协议实体按照前面的字段格式构造 trap 报告的 PDU，再将其发送出去。

(4)　SNMP PDU 的传输。

SNMP 的设计是独立于具体的传输网络的，也就是说，它既可以在 TCP/IP 的支持下操作，也可以在 OSI 的传输层协议支持下完成操作，甚至可以在以太网的直接支持下实现操作。其中对 OSI 传输层的服务没有要求，既可以是有连接的服务，也可以是无连接的服务。为了实现上述目标，Internet 组织定义了若干映射标准，规定了如何将 SNMP 协议数据单元 PDU 映射到下层的无连接传输请求上去。

在所有各种映射定义中，有一点是相同的，即所有 SNMP 报文数据是通过一个“顺序化”过程在网络上传输的，这个顺序化过程可以将任意结构的数据编码成一个有序的字符串进行传送。对方收到这些字符串后则按照完全相同的语法将它们解码成原来的数据结构。

(5)　MIB 中为 SNMP 定义的管理对象。

在 Internet 的第二版管理信息库(MIB-Ⅱ)中，为 SNMP 应用实体定义了若干管理对象，其中包括 SNMP 的各种服务原语、各种收发协议数据单元、各种参数指示或统计变量等，凡 SNMP 中可操作的数据结构或变量都包括在内，下面将详细介绍。

2. MIB-Ⅱ

在 TCP/IP 网络管理的建议标准中，提出了多个相互独立的 MIB，其中包含为 Internet 的网络管理而开发的 MIB-Ⅱ。鉴于它在说明标准 MIB 的结构、作用和定义方法等方面的重

要性和代表性，有必要对其进行比较深入的讨论。

MIB-Ⅱ是在 MIB-Ⅰ的基础上开发的，是 MIB-Ⅰ的一个超集。MIB-Ⅱ组被分为以下分组。

- system：关于系统的总体信息。
- interfaces：系统到子网接口的信息。
- at(address translation)：描述 Internet 到子网的地址映射。
- ip：关于系统中 IP 的实现和运行信息。
- icmp：关于系统中 ICMP 的实现和运行信息。
- tcp：关于系统中 TCP 的实现和运行信息。
- udp：关于系统中 UDP 的实现和运行信息。
- egp：关于系统中 EGP 的实现和运行信息。
- dot3(transmission)：有关每个系统接口的传输模式和访问协议的信息。
- snmp：关于系统中 SNMP 的实现和运行信息。

1) system 组

system 组提供有关被管系统的总体信息。

2) interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息。

3) address translation 组

address translation 组由一个表构成，表中的每一行对应系统中的一个物理接口，提供网络地址向物理地址的映射。一般情况下，网络地址是指系统在该接口上的 IP 地址，而物理地址决定于实际采用的子网情况。例如，如果接口对应的是 LAN，则物理地址是接口的 MAC 地址；如果对应 X.25 分组交换网，则物理地址可能是一个 X.121 地址。

实际上，address translation 组包含在 MIB-Ⅱ中只是为了与 MIB-Ⅰ兼容，MIB-Ⅱ的地址转换信息在各个网络协议组中提供。

4) ip 组

ip 组包含有关节点上 IP 的实现和操作的信息，如有关 IP 层流量的一些计数器。ip 组中包含 3 个表：ipAddrTable、ipRouteTable 和 ipNetToMediaTable。

ipAddrTable 包含分配给该实体的 IP 地址的信息，每个地址被唯一地分配给一个物理地址。

ipRouteTable 包含用于互联网路由选择的信息，该路由表中的信息是从一些协议的路由表中抽取而来的。实体当前所知的每条路由都有一个条目，表格由 ipRouteDest 索引。ipRouteTable 中的信息可用于配置的监测，并且由于表中的对象是 read-write 的，因此也可被用于路由控制。

ipNetToMediaTable 是一个提供 IP 地址和物理地址之间对应关系的地址转换表。除了增加一个指示映射类型的对象 ipNetToMediaType 之外，表中所包含的信息与 address translation 组相同。

此外，ip 组中还包含一些用于性能和故障监测的标量对象。

5)　icmp 组

ICMP(Internet Control Message Protocol)是 TCP/IP 协议族中的一部分，所有实现 IP 协议的系统都提供 ICMP。ICMP 提供从路由器或其他主机向主机传递消息的手段，它的基本作用是反馈通信环境中存在的问题。例如，数据报不能到达目的地，路由器没有缓冲区来转发数据报。

icmp 组包含有关一个节点的 ICMP 的实现和操作的信息，具体地讲，icmp 组为节点接收和发送的各种 ICMP 消息的计数器构成一个表。

6)　tcp 组

tcp 组包含有关一个节点的 TCP 的实现和操作的信息。

7)　udp 组

udp 组包含有关一个节点的 UDP 的实现和操作的信息。除了有关发送和接收的数据报的信息之外，这个组中还包含一个 udpTable 表，该表中包含 UDP 端点的管理信息。所谓 UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 表中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。

8)　egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)的实现和操作的信息。除了有关发送和接收的 EGP 消息的信息外，这个组中还包含一个 egpNeighTable 表，该表中包含有关相邻网关的信息。

3. RMON

简单网络管理协议 SNMP 是基于 TCP/IP 协议并在 Internet 中应用最广泛的网管协议，但是 SNMP 也有一些明显的不足，主要有以下 4 点。

- 由于 SNMP 使用轮询采集数据，而在大型网络中轮询会产生数量巨大的网络管理通信报文，导致网络交通拥挤甚至阻塞，故不适合管理大型网络。
- 不适合回收大信息量的数据，如一个完整的路由表。
- 基于 SNMP 的标准仅提供一般的验证，不能提供可靠的安全保证。
- 不支持 Manager-to-Manager 的分布式管理，它将收集数据的负担加在网管站上，使其成为瓶颈。

为了提高传送管理信息的可用性，减少管理站的负担，满足网络管理员监控网段性能的需求，IETF 开发了 RMON 以解决 SNMP 在日益扩大的分布式互联中的局限性。

远程网络监视(RMON)首先实现了对异构环境进行一致的远程管理，它为通过端口远程监视网段提供了解决方案。RMON 是 IETF 定义的 MIB(RFC1757)，是对 SNMP 标准的扩展，它定义了标准功能以及在基于 SNMP 管理站和远程监控者之间的接口，主要实现对一个网段乃至整个网络的通信流量的监视功能，目前已成为网络管理标准之一。它可以对数据网进行防范管理，使 SNMP 更有效、更积极主动地监测远程设备，使网络管理员可以更快地跟踪网络、网段或设备出现的故障，然后采取防范措施，防止网络资源的失效。RMON MIB 的实现可以记录网络事件，即使在网络管理站没有与监控设备主动进行连接(脱机)的情况下也如此。另外，RMON MIB 也用于记录网络性能数据和故障历史，可以在任何时候访问故障历史数据以进行有效的故障诊断。使用这种方法减少了管理者同代理间的通信流量，使

简单而有力地管理大型互联网络成为可能。

RMON 监视器可用两种方法收集数据：一种方法是通过专用的 RMON 探测仪，网管站直接从探测仪上获取管理信息并控制网络资源，这种方法可以获取 RMON MIB 的全部信息；另一种方法是将 RMON 代理直接植入网络设备(路由器、交换机、Hub 等)，使其成为带 RMON Probe 功能的网络设施，网管站用 SNMP 的基本命令与其交换数据信息，收集网络管理信息，但这种方式受设备资源的限制，一般不能获取 RMON MIB 的所有数据，大多只收集 4 个组的信息。

RMON MIB 对网段数据的采集和控制通过控制表和数据表来完成。RMON MIB 按功能分成 9 个组。每个组都有自己的控制表和数据表(有些组两者合一，如统计组)。其中，控制表可以读写，数据表只能读，控制表用于描述数据表所存放数据的格式。配置的时候，由管理站设置数据收集的要求，存入控制表。开始工作后，RMON 监视器根据控制表的配置，把收集到的数据存放到数据表中。

RMON MIB 包含以下 9 组数据。

1) 统计组

统计组(Statistics)统计被监控的每个子网的基本统计信息。网络管理员可以从 RMON 探针监测的设备端口获取一个网段的各种统计信息。目前只能对网络设备的以太网接口进行监控和统计，将来会扩展到包括更多接口的特定表格(如 FDDI)。它能统计一个网段的流量(如交通流量的总包数和总字节数)，统计各种类型包的分布(如广播包、多点广播包、不同大小包的数量)，还能统计各种类型错误包数、碰撞次数等。

2) 历史组

历史组(History)定期收集统计网络值的记录并为日后的处理把统计存储起来。它包含历史控制组和以太网历史组两个小组。其中历史控制组主要用来设置采样间隔时间等控制信息；以太网历史组为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

3) 警报组

警报组(Alarm)允许网络管理站为网络性能(可以是监视器本地 MIB 的任意整数类型的对象)定义一组报警阈值。如果阈值在相应的方向被越过，监视器就会产生警报并把警报发往网络管理站。警报组需要事件组的实现。

4) 主机组

主机组(Host)包含对连接在一个子网上所有主机的各种类型交通流量的记数值。它能够发现网上的新主机，对每个主机的 MAC 地址保持一组统计数据，例如，主机发送或接收的数据包总数、广播包数、流量字节数和错误包数等。它有一个控制表和两个数据表，且这两个数据表的内容相同，只是组织排列顺序不同。

5) 最高主机组

最高主机组(Host Top)包括排序后的主机统计，该报告基于主机表中的一些参数生成列表。它用于统计在一个子网上一些参数最高的一组主机，例如，它可以列出 10 个传输数据最多的主机，但依赖于主机组的实现。

6) 矩阵组

矩阵组(Matrix)用于记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储。

这种方法对于检索特定主机之间的流量信息十分有用，例如，用于找出哪些设备对服务器的使用最多。矩阵组由三个表组成：一个控制表和两个数据表。

7)　过滤组

过滤组(Filter)允许监视器观测与过滤器相匹配的数据包。网络监视器可以捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。

8)　包捕获组

包捕获组(Capture)控制数据被发往网管站的方式，它可以在把报文发送到某个通道后记录数据报文。

9)　事件组

事件组(Event)提供关于 RMON 代理所产生的所有事件的列表。当某个事件发生时可以记录日志和发送 IRAP 到网管站。

尽管 RMON 有很多优点，但也有其局限性。RMON 的 MAC 层探测器不能确定由服务器进入本地网段的数据包的源点和终点，或者不能确定经过被监视网段的通信数据包的源点和终点。

1994 年，RMON2 工作组开始致力于提高现存的物理层和数据链路层之间的 RMON 规范，以实现在网络层和应用层提供历史和数据的统计服务。图 1-14 说明了 OSI 参考模型与 RMON 相关规范的对应关系。

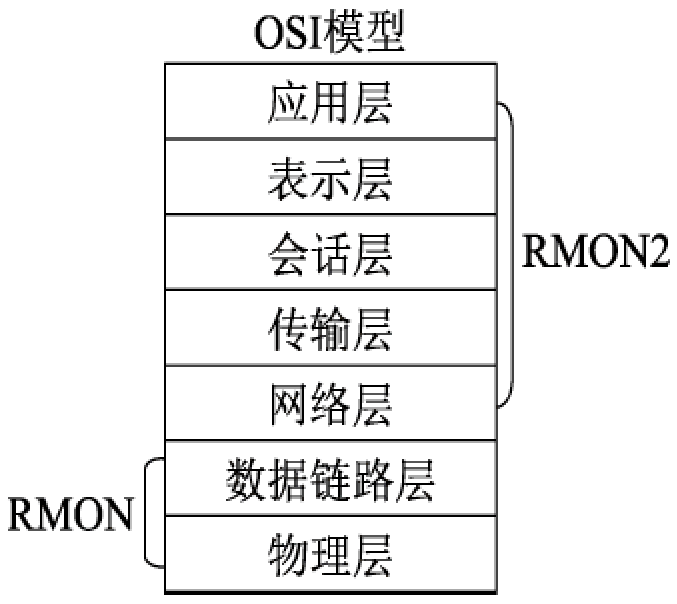


图 1-14　RMON 和 RMON2 所支持的协议层

在网络层，RMON2 通过监视点对点通信来记录网络使用的模式。另外，RMON2 还显示单个应用所占用的带宽，以及出现疑难故障的关键因素。

1.5.1.3　监视网络性能、故障和安全

1. 利用工具监视网络性能

网络性能信息收集方案包括以下几点。

- Internet 控制消息协议 ICMP Ping。
- 网络分析仪或探测仪。
- NetFlow。

1)　ICMP Ping

Ping 对网络专业人员来说是一个常用且对用户友好的故障排除技术。Ping 是一个工具，它使用 ICMP 返回请求和响应协议来测试与 IP 地址的连接性，能够快速浏览从工作站到目标 IP 地址的设备可达性和响应时间。然而，从工作站到远程节点使用 Ping 可能无法确定问题的位置，因为测量可能发生在不同网络路径或多跳上。此外，使用 ICMP 测量响应时间

不能准确反映应用的响应时间。一个透明、正常的网络(如具有快速 Ping 响应和低使用率的网络)可能仍然掩盖着潜在的响应时间问题，因为问题可能出在协议栈的上层中。

2) 网络分析仪或探测仪

网络分析仪或探测仪是监测和解决响应时间问题的常用工具。探测仪通常是一个用于监测网络段性能的专用硬件设备。例如，RMON2 探测仪可以分析现有网络业务并报告所连网络段的使用率、顶层会话者和会话，这些报告都被上层协议分开。探测仪可捕捉分组并分析分组的头信息，用于深入分析网络段的活动。

探测仪关于网络段利用率和错误数的报告可以帮助网络专业人员准确确定网络时延和问题。然而，需要在应用路径的每一跳上设置许多探测仪以检测网络时延所处的位置。尽管网络分析仪或探测仪可以得到有价值的信息，但在解决响应时间和可用性的问题上可能不是有效的方案。当校准网络或分析链路、协议和应用使用率趋势以及描述和识别最高层上的对话者和会话时，专用探测仪更合适。

3) NetFlow

Cisco IOS NetFlow 技术收集并测量进入特定路由器或交换机接口的数据，是 Cisco IOS 软件的一个组成部分。

通过分析 NetFlow 数据，网络管理人员能够确定拥塞的原因、每个用户的 CoS 以及应用，并确定业务的源网络和目的网络。NetFlow 支持极高的粒度和准确的业务测量以及高级聚合业务收集。由于它是 Cisco IOS 软件的一个组件，因此 NetFlow 支持基于 Cisco 产品的网络，以实现 IP 业务流分析，而无须购买客户探测仪，从而使大型 IP 网络上的业务分析更经济。

2. 利用工具监视网络故障

网络监视工具的种类较多，此处仅介绍 OpenView、NetView、SunNet Manager 和其他一些常用的监视工具。

1) HP 的 OpenView

HP 的 OpenView 是第一个真正兼容的、跨平台的网络管理系统，因此也得到了广泛的市场应用。虽然 OpenView 被认为是一个企业级的网络管理系统，但它跟大多数别的网络管理系统一样，不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。

OpenView 不能处理因为某一网络对象故障而导致的其他对象的故障。另外，在 OpenView 中，性能的轮询与状态的轮询是截然分开的，这样将导致一个网络对象响应性能的轮询失败，但不触发一个报警。只有当该对象不响应状态的轮询时才进行故障报警，这将导致故障响应时间的延长。

OpenView 还使用了商业化的关系数据库，这使得利用 OpenView 采集到的数据开发扩展应用变得相对容易。

2) IBM 的 NetView

NetView 既可以作为一个跨平台的、即插即用的系统提供给最终用户，也可以作为一个开发平台，在上面开发新的网络管理应用。它不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。NetView 产品系列包括一个故障卡片系统、一些新的故障诊断工具，以及一些 OpenView 所不具备的其他特性。

NetView 不能对故障事件进行归并，不能找出相关故障卡片的内在关系，因此对一个失效设备，即使是一个重要的路由器，也将导致大量的故障卡片和一系列类似的警报。因此，NetView 不具备在掌握整个网络结构情况下管理分散对象的能力。在一个大型、异构网络中，这意味着服务的开销不能轻易地从网络开销中区分出来。

同样地，在 NetView 中，性能轮询与状态轮询也是彻底分开的，这也将导致故障响应的延迟。NetView 也使用了商业化的关系数据库，这使得利用 NetView 采集来的数据开发扩展应用变得相对容易。

3)　Sun 的 SunNet Manager

SunNet Manager(SNM)是第一个重要的基于 UNIX 的网络管理系统。SNM 一直作为主要开发平台而存在，但它仅提供了很有限的应用功能。为了实用化，还必须附加很多第三方开发的针对具体硬件平台的网络管理应用。SNM 跟其他大多数网络管理系统一样，也不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。

SNM 有两个特性：Proxy 管理代理和集成控制核心。

4)　其他常用工具

网络故障检测还经常用到一些命令，如 ping、traceroute、nslookup、netstat、arp 以及 route 等。

(1)　ping 命令。

ping 命令是网络中使用最频繁的测试命令，它的协议基础是 TCP/IP 协议中的 ICMP。

ping 命令发出 ICMP 的 Echo 消息，接收者听到后应答 ICMP 的 Echo 应答消息，这一问一答就表明源站与目的站间的 TCP/IP 协议可以进行正常的连通。ping 命令还具有测试网络响应时间的功能，以问答间隔为标准。配置管理中网络拓扑图的自动发现就是通过 ICMP 协议以类似于 ping 命令的方式完成。

(2)　traceroute 命令。

traceroute 命令用来测试 IP 数据包到达目的端经过的所有路由器的路径及连通状况，它通过每一个路由器的响应时间来反映速度快慢，在测试路由协议的配置时经常使用。

(3)　netstat 命令。

netstat 命令是显示 TCP/IP 协议状态的命令，工作站中的网络问题用此命令进行分析。

(4)　nslookup 命令。

nslookup 命令用于向 DNS 服务器发送一个 DNS 查询，对完整的域名和 TCP/IP 地址进行查询解析，然后显示 DNS 服务器的名称、地址和解析到的信息。

(5)　Cisco Management Station to Device 工具。

如果一个设备可以对 ping 或者 traceroute 命令进行响应，但是却不能支持 SNMP 或者其他第 4 层的应用，则可以使用 Cisco Management Station to Device 工具来测试应用方面的问题。这个工具可以用来测试 UDP、TCP、HTTP、TFTP、Telnet 和 SNMP 的连接是否正常。对于 UDP 和 TCP，所测试的端口为 7，对于其他的协议，将测试服务器一侧的端口。对于各个应用来说，这个工具就像是一个客户端。为了取得测试成功，在设备上必须运行以上提及的协议，将之作为一个 Server。例如，为了取得 HTTP 测试的成功，需要使用 ip http server 命令在路由器上启动 Web 接口。如果使用的是主机名而不是 TCP/IP 地址，则在测试

之前将首先对主机名进行解析并将解析的结果显示出来。

(6) Network Show Command 应用。

Network Show Command 应用是一个基于 Java 的工具，通过这个工具，管理员可以定义用户针对其 Cisco 设备运行的 show 命令列表。Network Show Command 还提供了一个可选的远程控制台选项，在这个控制台上，可以输入 show 命令列表中没有定义的 show 命令。

Network Show Command 工具存在的问题是它的权限控制操作十分复杂，权限严格限制了用户可以执行的命令，但是并不限制它能够完成的功能。当把 Network Show Command 工具和 NetConfig 工具一起使用的时候，用户只有有限的特权，只能配置网络设备上的某些属性，根据 NetConfig 应用中的模板来修改设备的配置，这些模板是由管理员创建的。用户通过 Network Show Command 工具，可以验证 NetConfig 任务的输出结果。另外一个优点是 Network Show Command 工具和 NetConfig 工具可以一次性对多个设备产生影响，比较高效。

3. 利用工具监视网络安全

1) 入侵检测系统

入侵检测系统是近几年出现的新型网络安全技术，它试图发现入侵者或识别出对计算机的非法访问行为，并对其进行隔离。入侵检测系统能发现其他安全措施无法发现的攻击行为，并能收集可以用来诉讼的犯罪证据。

入侵检测系统有两类：基于网络的实时入侵检测系统和基于主机的实时入侵检测系统。目前 IDS 解决方案和产品有很多种，这里介绍的入侵检测产品为 Cisco 的 IDS。

2) Cisco IDS 解决方案

考虑到企业站点非常复杂，攻击技术多种多样，黑客数量只增不减，必须采用全面的解决方案才能有效预防黑客袭击。这种解决方案应该能对抗多种攻击技术，并防止在典型攻击过程中执行的恶意操作。由于 Cisco IDS 解决方案提供包含 NIDS 和 HIDS 组件的组合解决方案，因而能满足这个要求。NIDS 主要用于预防网络袭击，而 HIDS 则主要用于防止服务器的 OS 操作系统和应用遭受袭击。

NIDS 检测器可以安装在多个位置上，最重要的位置是防火墙的前面，负责监控进入机构的通信信息。另外，每个重要的网段都安装一个检测器。HIDS 首先部署在面对互联网的服务器上，例如 Web、邮件和 DNS 服务器。由于面向互联网的服务器与后端服务器相连，因此，HIDS 也部署在公司防火墙内的所有其他主要服务器上。

(1) Cisco IDS 网络检测器。

Cisco IDS 网络检测器能够为网络设备及服务器上的通信模块提供全面保护。其主要特性如下。

- 积极响应(系统包含对检测器设备的主动响应功能)。
- 全面检测网络袭击。
- 全面检测应用袭击。
- 以独特的方式预防拒绝服务攻击(Deny of Services，DoS)。
- 先进的 IP 分片重装和 Whisker 反 IDS 检测功能支持。

(2) Cisco IDS 主机检测器。

Cisco IDS 主机检测器能够为服务器上运行的服务器操作系统和应用提供全面保护。主机检测器安装在每台服务器上，用于保护操作系统和应用。系统利用呼叫截获技术提供纯

主动式服务器安全系统。其主要特性有以下几个。

- 现场预防操作系统和应用袭击。
- 防止缓冲器溢出袭击。
- 不断提高完整性。
- Web 服务器屏蔽。
- 防止安全套接层(SSL)加密的 HTTP 袭击。

3)　漏洞扫描安全评估技术

漏洞扫描安全评估技术可以帮助网络管理者对网络的安全现状进行扫描，并在发现漏洞后提出具体的解决办法。

网络安全漏洞扫描系统通常安装在一台与网络有连接的主机上。系统中配有一个信息库，其内存放着大量有关系统安全漏洞和黑客攻击行为的数据。扫描系统根据这些信息向网络上的主机和网络设备发送数据包，观察被扫描的设备是否存在与信息库中记录的内容相匹配的安全漏洞。扫描的内容包括主机操作系统本身、操作系统的配置、防火墙配置、网络设备配置以及应用系统等。

通过网络扫描，系统管理者可以及时发现网络中存在的安全隐患，并进行必要的修补，从而减小网络被攻击的可能性。

(1)　安全扫描方式。

安全扫描方式包括直接配置检查和模拟入侵两种。

- 直接配置检查：这种技术的代表是 COPS(Computer Oracle Password and Security System)。COPS 从系统内部常见的 UNIX 安全配置错误与漏洞(如关键文件权限设置、FTP 权限与路径设置、root 路径设置、密码等)入手，指出系统内存在的安全问题，从而减少系统可能被入侵者(包括内部用户)利用的漏洞。
- 模拟入侵：这种技术模拟入侵者可能的攻击行为，从系统外部进行扫描，以探测是否存在可以被入侵者利用的系统安全的薄弱之处。其代表有 ISS(Internet Security Scanner)和 SATAN(Security Analysis Tool for Auditing Network)。

(2)　安全扫描工具。

安全扫描工具通常分为基于服务器和基于网络的扫描器。

基于服务器的扫描器主要扫描与服务器相关的安全漏洞，如 password 文件、目录和文件权限、共享文件系统、敏感服务、软件、系统漏洞等，并给出相应的解决办法建议。该类扫描器通常与相应的服务器操作系统紧密相关。

基于网络的安全扫描器主要扫描设定网络内的服务器、路由器、网桥、交换机、访问服务器、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力。通常该类扫描器限制使用范围(IP 地址或路由器跳数)。

4. 性能监视的检查点

网络性能包括带宽利用率、吞吐率降低的程度、通信繁忙的程度、网络瓶颈及响应时间等，这些参数的控制和优化是系统管理人员的日常性工作。性能指标通过性能监测设备采集并存储在数据库中。数据库可以放在代理中，也可以放在管理站中，这取决于代理和管理站的能力以及通信开销的大小。

如果数据量太大，可以只存储统计摘要和趋势分析的结果。在 ISO 10165—2(管理信息定义)中定义的管理对象的某些属性代表了系统的性能参数。这些属性如下所述。

- 计数器(Counter)。计数器的特点是初始值为零，其值只能增加不能减少，增加到最大值时归零。它的应用很广泛，例如，可以用来表示工作站接收的分组数。
- 计量器(Gauge)。与计数器不同，计量器的值可增加也可减少，达到最大值时不归零，而是不再增加，但可以减少。例如，可以用它表示网络层实体管理的队列长度。
- 阈值(Threshold)。阈值可用于计数器或计量器。当计数器的值达到某个阈值时管理对象要发出通知。计量器的阈值有两个，分别是上限和下限，并且仅当被监视的量的变化经过上/下限时，管理对象才发出报警通知。
- 涨潮点(Tidemark)。涨潮点是指计量器的最低点或最高点。涨潮点的属性有 3 个值，即当前值、最近一次复位之前的值和最近复位的时间等。后两个值可用来计算潮汐的大小和到达涨潮点的时间。

5. 系统性能分析

性能分析功能要完成以下任务。

- 对监测到的性能数据进行统计和计算，获得网络及其主要元素的性能指标，定期产生性能报表。
- 负责维护性能 MIB，存储网络及其主要元素性能的历史数据。
- 根据当前数据和历史数据对网络及其主要元素的性能进行分析，获得性能的变化趋势，分析制约网络性能的瓶颈问题。
- 在网络性能异常的情况下向网络管理者进行警告，在特殊情况下，直接启动故障管理功能进行反应。

性能分析的基础是建立和维护一个有效的性能 MIB。在此基础上，要解决的关键问题是设计和构造有效的性能分析方法。传统的方法是基于解析的方法。

解析的方法又分为预测法和解释法两种。预测法是根据网络的结构以及各个网络元素的性能，推测网络的总体性能的方法。解释法是从网络的结构以及观测到的总体性能出发，推测各个网络元素性能的方法。由于解析的方法具有局限性，因此对于比较复杂的关系难以迅速得到正确结果。

现在，基于人工智能的网络性能分析方法越来越受到重视。在这种方法中，一般利用专家系统对网络性能进行分析，提高了分析的水平和速度。

6. 安全监视的检查点

安全管理的目的是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据以及系统免受侵扰和破坏。目前采用的网络安全措施主要包括通信伙伴认证、访问控制、数据保密和数据完整性保护等。一般的安全管理系统包含风险分析功能，安全服务功能，报警、日志和报告功能，网络管理系统保护功能等。

需要明确的是，安全管理系统并不能杜绝所有对网络的侵扰和破坏，其作用仅在于最大限度地防范，以及在受到侵扰和破坏后将损失尽量降低。具体地说，安全管理系统的主要作用有以下几点。

- 采用多层防卫手段，将受到侵扰和破坏的概率降到最低。
- 提供迅速检测非法使用和非法入口的手段，核查跟踪侵入者的活动。
- 提供恢复被破坏的数据和系统的手段，尽量降低损失。
- 提供查获侵入者的手段。

1.5.1.4　故障恢复分析

1. 故障分析要点

故障定位是在一个给定的系统中检测、隔离和修理故障的过程。

一个网络是一个动态系统，对于一个动态的系统而言，故障定位的主要挑战在于，如何在许许多多的部件中隔离出故障部件。有经验的故障定位人员和网络技术人员遵循一套精心设计的过程来诊断一个问题的来源。

进行故障定位所遵循的规则实际上是在基于一些常识的基础上进行的，例如：

- 确定问题的实际性质。
- 隔离问题的原因。
- 解决问题。

“确定—隔离—解决”这 3 个步骤在大部分网络中都能够成功地奠定对问题故障定位的基础，如图 1-15 所示。

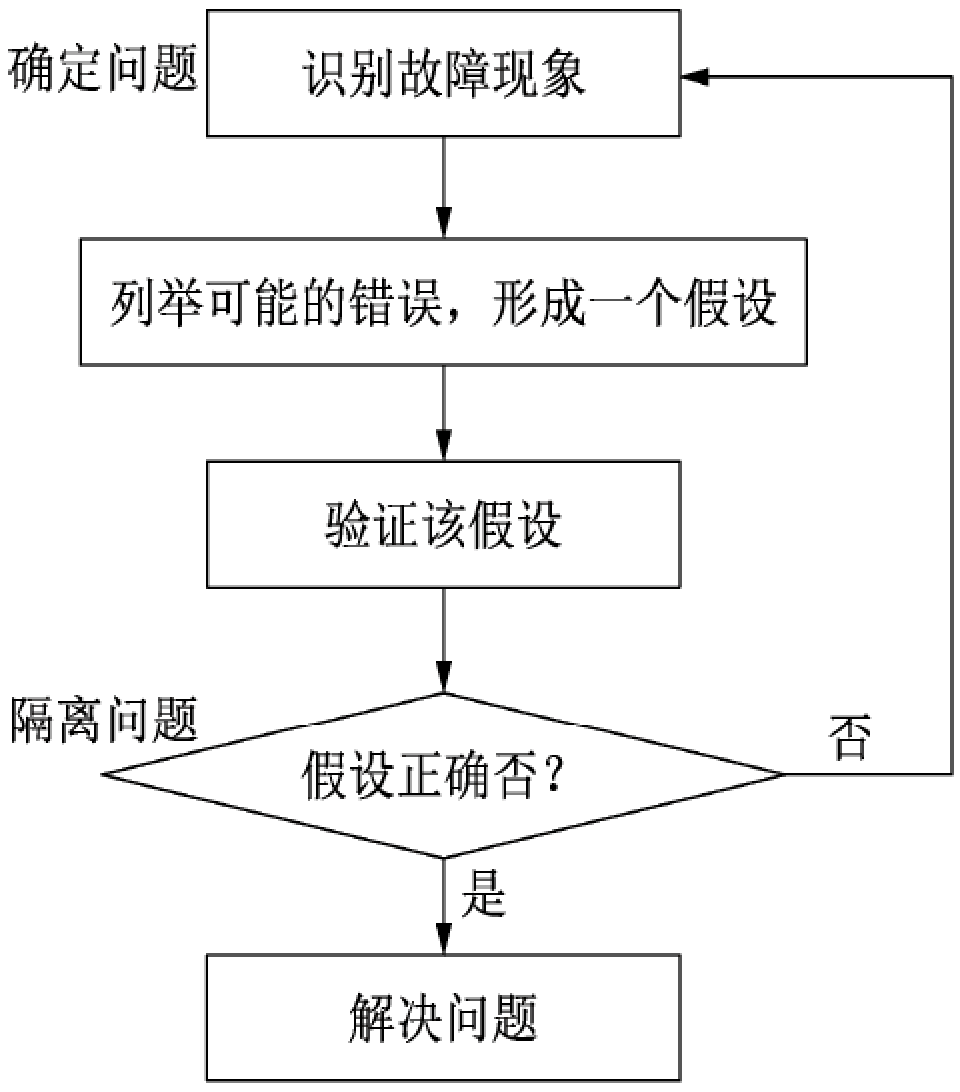


图 1-15　诊断网络问题的循环过程

1)　识别故障现象

知道出了问题并能够避免，是进行成功故障定位最重要的步骤。大部分网络问题是通过某些现象表现出来的。所以在遇到问题时，要想高效地解决问题，首先必须能对问题进行定位，这就需要设法收集一些与问题有关的线索。需要强调的一点是，在确定问题的实际性质之前，必须知道系统的正常运行特性(即基线)。

2)　对故障现象进行详细描述

如果得到一个差错消息，应将屏幕显示的内容记录下来，并将该差错信息写到一个网络差错日志中。差错消息的内容以及差错显示的位置(是显示在服务器上还是显示在客户机

上)信息，对于判断该差错发生的位置是一个重要的线索。

所以，一定要在网络配置日志中对每个硬件和软件的改变做详细的记录。一旦把能够观察到的一切现象都收集到了，就可以依赖经验形成一个假设。

3) 列举可能的错误并形成假设

列举出所有可能导致被监测到的故障现象，然后利用有效的工具剔除各种可能的误报故障，根据最终结果形成一个关于故障的假设。

在故障定位中，经验和专门知识是非常有用的。为了使假设与这些现象相一致，必须熟悉网络问题的类型，才能从正常出现的网络问题中分辨出这些故障现象，同时也需要深入理解运行在该网络上的相关协议和应用程序。

4) 隔离问题的来源

确定问题可能的来源后，应该针对不同原因分别进行测试。当决定这样做时，应当能够确定假设的正确性。

5) 验证假设

可以使用几种方法来验证假设的正确性。专家们经常使用的一种方法是“替换法”，即用可以正常工作的类似部件来替代怀疑存在问题的部件。在熟悉每个部件的性能以及它们可能引起的后果时，使用这个方法比较有效。

6) 得出结论

针对每个假设进行的实验，必须确定该假设是否正确。如果问题依然存在，则可判断该假设是不正确的。如果问题已经解决了，则表明已经找到了问题的根源。其中最麻烦的一种情况是，当替换掉部件之后，问题依然存在，但外在表现形式却不同。随着积累的经验越来越多，将逐渐知道对于每个可能的实验的结果，其结论会是什么。对于一个具有可能不熟悉的测试结果的实验，应该扩展或修订关于该问题的方法，从而能够更好地将所观察到的测试结果与收集到的现象联系在一起。

故障的定位过程是一个循环的过程。如果一个测试的结果没有得出结论，必须重新详细地分析该问题所表现出的现象，从而形成新的假设。在大多数情况下，需要在重新检查该现象之前，变换一下该问题的环境。

7) 解决问题

一旦隔离出所有故障的部件后，必须对此故障进行修复。围绕有问题的部件进行修理、更换或处理。对于有故障的硬件，唯一的选择就是修理或更换该部件。对于软件，通常可以通过重新安装或删除来修复该问题。

2. 网络监视器

一旦发现了用户错误或物理连接问题(包括网线损坏)，一些网络监控工具(包括网络监视器和分析仪)就会帮助分析网络流量、捕捉和分析网络上的数据，进行一个更深入的分析。

网络监视器是一个基于软件的工具，它可以在连到网络上的一台服务器或工作站上持续监测网络流量。网络监视器一般工作在 OSI 模型的第三层，可以检测出每个包使用的协议，但是不能破译包里的数据。

网络分析仪是一个便携的、基于硬件的工具。网络管理员把它连入网络，专门用来解决网络问题。网络分析仪可以破译直到 OSI 模型第七层的数据，例如，分析仪可以辨别一

个使用 TCP/IP 的包，甚至可以辨别它是从特定工作站到服务器的 ARP 应答信号。分析仪可以破译包的负载率，把它从二进制码转换为易读的十进制或十六进制码，因此，网络分析仪可以捕获运行于网络上的密码(只要它们的传输不是加密的)。一些网络测试仪软件包可以在标准 PC 上运行，但有的需要在带特殊网络接口卡和操作系统软件的 PC 上运行。

网络监视工具通常比网络分析仪便宜，并且可能包含在网络操作系统软件中，下面介绍其中的两种：Microsoft 的 Network Monitor(附于 Windows NT Server Version 4.0 及以后系统)和 Novell 的 LANalyzer agent(附于 Novell's manage wise software package)。其他的产品有类似的工作方式，大多数甚至使用非常相似的图形界面。

注意：为了利用基于软件的网络监视器和分析仪，计算机上的网络接口卡必须支持随机模式。随机模式是指设备驱动程序引导网络接口卡接收流过网络的所有帧，不光是指向该节点的帧。

1) 微软的网络监视器

Network Monitor(NetMon)是基于软件的且内置于 Windows NT Server 4.0 或者 Microsoft 的 Systems Management Server(SMS)的网络监视软件。它提供以下功能。

- ◆ 从一段或几段网络中捕获传输数据。
- ◆ 捕获来/去特殊节点的帧。
- ◆ 通过发送指定数量和类型的数据重现网络状态。
- ◆ 检测在网络上 NetMon 的其他运行副本(依赖于路由器的位置和配置)。
- ◆ 产生网络活动的参数。

NetMon 最有用的能力是捕获网络上传输的数据，NetMon 观察网络一段时间后，捕获通过特定网络的数据(因为 NetMon 利用随机模式，它捕获所有的数据，不仅仅是来/去 NetMon 控制台的数据)。然后，可以在 NetMon 中找出错误的帧，按照每个节点产生坏数据的多少按从大到小的顺序排序，一般在队列最前边的工作站就是问题所在，在网络传输中，它产生了比其他节点多得多的坏数据包。

2) Novell 的网络分析仪

Novell 提供了一个和 Microsoft 的 Network Monitor 相似的网络监视工具——LANalyzer 代理，它可作为一个独立的程序工作于 Windows 工作站或作为 Manage Wise 的一部分在 Netware 服务器上装配网络管理工具。LANalyzer 具有如下功能。

- ◆ 能发现网段上几乎所有的网络节点。
- ◆ 连续监测网络流量。
- ◆ 当流量达到预定的阈值时报警(例如利用率超过 70%)。
- ◆ 捕获来(或去)所有(或选定)节点的流量。

像 Network Monitor 一样，LANalyzer 能按节点捕获流量和辨别错误数据，按网段产生流量参数；另外，作为 Manage Wise 的套件，LANalyzer 能在特定的网段上发现所有的节点。它可以利用这些数据构造网络管理系统，这个网络管理系统不仅可以收集信息(例如，发现一个用户在某一特定的工作站上登录的次数，记录工作站通向服务器申请程序的类型)，而且可以提供实时的网络参数，当达到网络阈值时发送提示信息或发出警告声音。

3. 网络分析软件

除了利用随同网络操作系统的软件，还可以从专门从事网络管理的提供商那里购买网络分析软件。一个典型的例子是网络联盟的 NetXRay，这个网络分析软件提供数据捕获、分析、发现节点、流量转向、记录、报警和利用率预测。NetXRay 与 Network Monitor 和 LANalyzer 有相同的特征，同时又增加了一些附属物，它也可以为了重现网络故障而产生流量和同时监测多个网络段，其图形界面使这个产品使用方便，显示网络流量的可读性强。NetXRay 支持多协议和网络拓扑结构。

另外，网络联盟还牵头开发了基于硬件的网络分析仪，叫作探测器(Sniffer)。探测器通常是装配了特殊的网络接口卡和网络分析软件的便携式电脑。探测器的基本工作是分析网络问题。探测器提供了它所能捕获到的大量的各种类型和深度的信息。用这种类型工具的危险是它可能收集了超过计算机所能处理的信息，为了避免这个问题，应该为收集到的数据设置过滤器。

如果一个网络是全部交换的(即每个节点连接到自己的交换端口)，则网络分析仪只能捕获到广播的包和目的地址为正运行软件的节点的包，因为在交换环境下，只有这些数据包才能传输到目的地址。交换机的使用使网络监视更加困难，解决方案是重新配置交换机以重新选择路由，这样网络分析仪才能接收到所有的流量。显然，应该权衡一下重新配置引起的破坏性和潜在的好处(能够分析网络流量和排除故障)。

4. 排除故障要点

网络故障排除应按照规定的步骤进行，这样可以节省时间和经费(譬如不必要的软件、硬件替换等)。

1) 网络排错的步骤

网络排错的步骤如下。

(1) 认清症状。

(2) 验证用户权限。例如，确保用户正确地输入了口令。

(3) 限定问题的范围。它是全局性的吗？即网上的所有用户总是会碰到这个问题吗？或者问题只发生在网络上某一地理区域、某一特定的工作组、某一特定的时间段？换句话说，这问题是属于地区性的、工作组性的还是时间相关的?

(4) 重现故障，并且要保证能够可靠地重新产生这个错误。

(5) 验证网络物理连接(例如网络连线、网络接口卡的插槽、供电电源)的完整性。从受到影响的节点开始，向主干网延伸。

(6) 验证网络的软连接问题(例如地址、协议绑定、软件安装等)。

(7) 考虑最近的网络变更和可能因此导致的网络问题。

(8) 实施解决方案。

(9) 检验解决方案。

根据自己的观察，可以从上述步骤中的一步跳到另一步，以减少所执行的检查步骤。

2) 故障查找注意事项

由于以太网采用通用总线拓扑结构以及物理层可扩展的潜在问题，所以某个特定物理层的问题会以不同的方式显示出来，而且由于采用的测试手段、位置和环境不同，显示出

的现象还常常相互矛盾。

为了避免被假象所误导，可以按照以下两个步骤查找故障。

(1) 沿网段多做几次测试。

如果故障现象随测试点的不同还保持一样，就可以依照所测试出的故障现象去排除。如果故障现象在一些或所有的测试点都不相同，就要把查找故障的方向定在物理层(除非有特别提示)，例如，查找坏的电缆、噪声环境、接地循环等故障。

(2) 要提高测试质量。

在测试的同时要把测试仪器设置成至少可同时发送较低的流量。由于增加了网络流量，微小的和间歇性的物理层问题就会暴露出来。

5. 网络故障诊断和排除

网络中可能出现的故障多种多样，解决一个复杂的网络故障往往需要广泛的网络知识与丰富的工作经验。这也是为什么一个成熟的网络管理机构制定有一整套完备的故障管理日志记录机制，同时人们也率先把专家系统和人工智能技术引进到网络故障管理中来的原因。另外，由于网络故障的多样性和复杂性，网络故障的分类方法也不尽相同。

1) 按照故障性质分类

根据网络故障的性质可以把故障分为物理故障与逻辑故障。

(1) 物理故障。物理故障是指设备或线路损坏、插头松动、线路受到严重电磁干扰等的情况。比如，网络中某条线路突然中断，这时网络管理人员从监控界面上会发现该线路流量陡然下降或系统弹出报警界面，此时首先用 ping 检查线路在网络管理中心的端口是否连通。如果不连通，则检查端口插头是否松动，如果松动则插紧，再用 ping 检查，如果连通则故障解决。这时需把故障的特征及其解决步骤详细记录下来。也有可能是线路远离网络管理中心的那端插头松动，此时则需要通知对方进行解决。另一种常见的物理故障就是网络插头误接。这种情况经常是在没有搞清网络插头规范或没有弄清网络拓扑规划的情况下导致的。另一种情况，比如两个路由器直接连接，这时应该让一台路由器的出口连接另一台路由器的入口，而这台路由器的入口连接另一台路由器的出口才行，这时制作的网线就应该满足这一特性，否则也会导致网络误接。不过像这种网络连接故障显得很隐蔽，要诊断这种故障没有什么特别好的工具，只能依靠经验。

(2) 逻辑故障。逻辑故障中的一种常见情况是配置错误，就是指因为网络设备的配置原因而导致的网络异常或故障。配置错误可能是路由器端口参数设定有误，或路由器的路由配置错误以至于路由循环或找不到远程地址，或者是网络掩码设置错误等。比如，同样是网络中某条线路故障，发现该线没有流量，但又可以 ping 通线路两端的端口，这时很可能就是路由配置错误导致循环了。诊断该故障可以用 traceroute 工具，可以发现在 traceroute 的结果中某一段之后，两个 IP 地址循环出现。这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 地址在该线路上来回反复传递。这时需要更改远端路由器端口配置，把路由设置为正确配置，就能恢复线路了。当然处理该故障的所有动作都要记录在日志中。

逻辑故障中另一类故障就是一些重要进程或端口关闭，以及系统的负载过高。比如，路由器的 SNMP 进程意外关闭或死掉，这时网络管理系统将不能从路由器中采集到任何数据，因此网络管理系统失去了对该路由器的控制。还有，就是线路中断，没有流量，这时

用 ping 发现线路近端端口 ping 不通，检查发现该端口处于 down 的状态，就是说该端口已经关闭了，因此导致了故障。这时只需重新启动该端口，就可以恢复线路的连通了。

2) 按照故障对象分类

根据故障的不同对象可将网络故障划分为线路故障、路由器故障和主机故障。

(1) 线路故障。线路故障最常见的情况就是线路不通。诊断这种故障可用 ping 检查线路远端的路由器端口是否还能响应，或检测该线路上的流量是否还存在。

一旦发现远端路由器端口不通，或该线路没有流量，则表示该线路可能出现了故障。这时有几种处理方法。

首先是 ping 线路两端的路由器端口，检查两端的端口是否关闭了。如果其中一端端口没有响应，则可能是路由器端口故障。如果是近端端口关闭，则可检查端口插头是否松动，路由器端口是否处于 down 的状态；如果是远端端口关闭，则要通知线路对方进行检查。进行这些故障处理之后，线路往往就通畅了。

如果线路仍然不通，一种可能就是通知线路的提供商检查线路本身的情况，看是否线路中间被切断等。另一种可能就是路由器配置出错，比如路由循环了。就是远端端口路由又指向了线路的近端，这样线路远端连接的网络用户就不通了，这种故障可以用 traceroute 来诊断。解决路由循环的方法就是重新配置路由器端口的静态路由或动态路由。

(2) 路由器故障。事实上，线路故障中很多情况都涉及路由器，因此也可以把一些线路故障归结为路由器故障。但线路涉及两端的路由器，因此在考虑线路故障时要涉及多个路由器。而有些路由器故障仅仅涉及它本身，这些故障比较典型的就是路由器 CPU 温度过高、CPU 利用率过高和路由器内存余量太小。其中最危险的是路由器 CPU 温度过高，因为这可能导致路由器被烧毁。而路由器 CPU 利用率过高和路由器内存余量太小都将直接影响网络服务的质量，比如路由器上的丢包率就会随内存余量的下降而上升。

检测这种类型的故障，需要利用 MIB 变量浏览器工具，从路由器 MIB 变量中读出有关的数据。通常情况下，网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。而解决这种故障，只有对路由器进行升级、扩内存等，或者重新规划网络的拓扑结构。另一种路由器故障就是自身的配置错误，比如配置的协议类型不对、配置的端口不对等。这种故障比较少见，没有什么特别的发现方法，排除故障就与网络管理人员的经验有关了。

(3) 主机故障。主机故障常见的现象就是主机的配置不当。比如，主机配置的 IP 地址与其他主机冲突，或 IP 地址根本就不在子网范围内，这将导致该主机不能连通。还有一些服务的设置故障，比如邮件服务器设置不当导致不能收发 E-mail，或者 DNS 服务器设置不当将导致不能解析域名。主机故障的另一种可能是主机安全故障，比如主机没有控制其上的 finger、rpc 和 rlogin 等多余服务。而恶意攻击者可以通过这些多余进程的正常服务或错误(Bug)攻击该主机，甚至得到该主机的超级用户权限等。

另外，还有一些其他的主机故障，比如共享本机硬盘不当等，将导致恶意攻击者非法利用该主机的资源。发现主机故障是一件困难的事情，特别是别人恶意的攻击。一般可以通过监视主机的流量、扫描主机端口和服务来防止可能的漏洞。当发现主机受到攻击之后，应立即分析可能的漏洞，并加以预防，同时及时通知网络管理人员注意。

6. 故障报告撰写要点

网络出现故障问题长期解决不了，就要建立一个单独文档记录所有的发现问题、解决问题的信息。这个问题档案的序号要记录到工作日志中以便交叉查询，项目结束后它应当记录了很多问题以及解决问题所需要的技术信息。

故障报告是反映网络系统出现故障情况及解决方法的文档，文档可以只是简单的文本形式，一页通常记录一个问题；可以使用数据库，这样便于交叉查找。表 1-3 所示为故障报告的一个简单样本，建立它或使用它都非常节省时间。

表 1-3　故障报告样本

故障报告 **状态**　　　　　　　　　　　　　　　　序号________ 报告________日期________测试人________日期________ 修复________日期________测试人________
关键操作参考：
故障描述：
故障解决：

项目结束后，这份文档要加入历史文档，供其他项目或其他组织使用。经常做这样的工作，测试的成本就会随项目的不断进行而下降。

1.5.1.5　危害安全的对策

1. 危害安全情况分析

风险分析是安全管理系统需要提供的一个重要功能。它要连续不断地对网络中的消息

和事件进行检测，对系统受到侵扰和破坏的风险进行分析。风险分析必须包括网络中所有有关的成分。

进行风险分析的一个方法是构造威胁矩阵，显示各个部分潜在的非攻击性或攻击性威胁。表 1-4 给出了一个威胁矩阵的例子。

表 1-4　威胁矩阵示例

<table>
<tr><th colspan="2" rowspan="2">威胁对象</th><th colspan="3">非攻击性威胁</th><th colspan="5">攻击性威胁</th></tr>
<tr><th>盗听通话</th><th>盗听数据</th><th>分析业务流</th><th>重复信息</th><th>修改信息</th><th>插入信息</th><th>伪造身份</th><th>拥塞网络</th></tr>
<tr><td colspan="2">端点用户</td><td>H</td><td>M</td><td>L</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td rowspan="2">交换机</td><td>电缆</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>光缆</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>M</td><td>M</td></tr>
<tr><td rowspan="2">本地网</td><td>电缆</td><td>L</td><td>L</td><td>M</td><td>L</td><td>L</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>光缆</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>M</td><td>M</td></tr>
<tr><td rowspan="4">长途网</td><td>电缆</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td><td>M</td><td>H</td></tr>
<tr><td>微波</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td><td>M</td><td>M</td></tr>
<tr><td>光缆</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>L</td><td>M</td><td>L</td></tr>
<tr><td>卫星</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td rowspan="3">软件</td><td>操作系统</td><td>L</td><td>L</td><td>L</td><td>M</td><td>M</td><td>L</td><td>M</td><td>M</td></tr>
<tr><td>数据库</td><td>L</td><td>L</td><td>L</td><td>M</td><td>M</td><td>M</td><td>M</td><td>M</td></tr>
<tr><td>应用</td><td>M</td><td>M</td><td>M</td><td>H</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
</table>

注：表中 H 表示高度威胁，M 表示中度威胁，L 表示低度威胁。

通常，非攻击性威胁包括以下几个。

◆ 盗听通话。目的是识别通话双方，获取秘密信息。
◆ 盗听数据。目的是获取口令等秘密信息。
◆ 分析业务流。获取业务量特征，以便进一步进行侵扰破坏。

在大多数情况下，非攻击性威胁是可以防范的，而攻击性威胁却不能完全防范，常常会引起较严重的后果。攻击性威胁包括以下几个。

◆ 重复信息。重复或阻延信息的传送，以迷惑和干扰信息的接收者。
◆ 插入信息。插入或删除传输中的信息，使信息接收者产生错误的反应。
◆ 拥塞网络。通过播放大量的信息拥塞传输系统，阻止网络中信息的正常传送。
◆ 修改信息。对关键数据(如账号)进行修改，引起网络管理的混乱。
◆ 伪造身份。使用伪造的身份标识进入网络，访问无权访问的信息，进行非法操作。

网络可以采用的安全服务多种多样，但是没有哪一个服务能够抵御所有的侵扰和破坏，只能通过对多种服务进行合理的组合来获得满意的网络安全性能。网络安全服务是通过网络安全机制来实现的。OSI 系统管理标准中定义了 8 种网络安全机制，它们是加密、数字签名、访问控制、数据完整性、认证、伪装业务流、路由控制以及公证。

网络管理系统提供的安全服务可以有效地降低安全风险，但它们并不能排除风险。

与故障管理相同，安全管理也要提供报警、日志和报告功能。该功能要以大量的侵扰检测器(可以由软件实现)为基础。在发现侵入者进入网络时触发报警过程，登录安全日志和向安全中心报告发生的事件。在报警报告和安全日志中，主要应包括以下信息。

- 事件的种类。
- 发生的时间。
- 事件中通信双方的标识符。
- 有关的资源标识符。
- 检测器标识符。

2. 防火墙技术

防火墙是一种特殊的设备(通常是一个路由器，也可能只是一台运行专用软件的 PC)，它有选择地过滤或阻塞网络间的流量。通常防火墙都是硬件和软件的结合(如路由器的操作系统和配置)，它可能位于两个互相连接的私有网络处，更常见的是在一个私有网络与一个公共网络(比如 Internet)连接处。图 1-16 所示为常见防火墙的示意图。

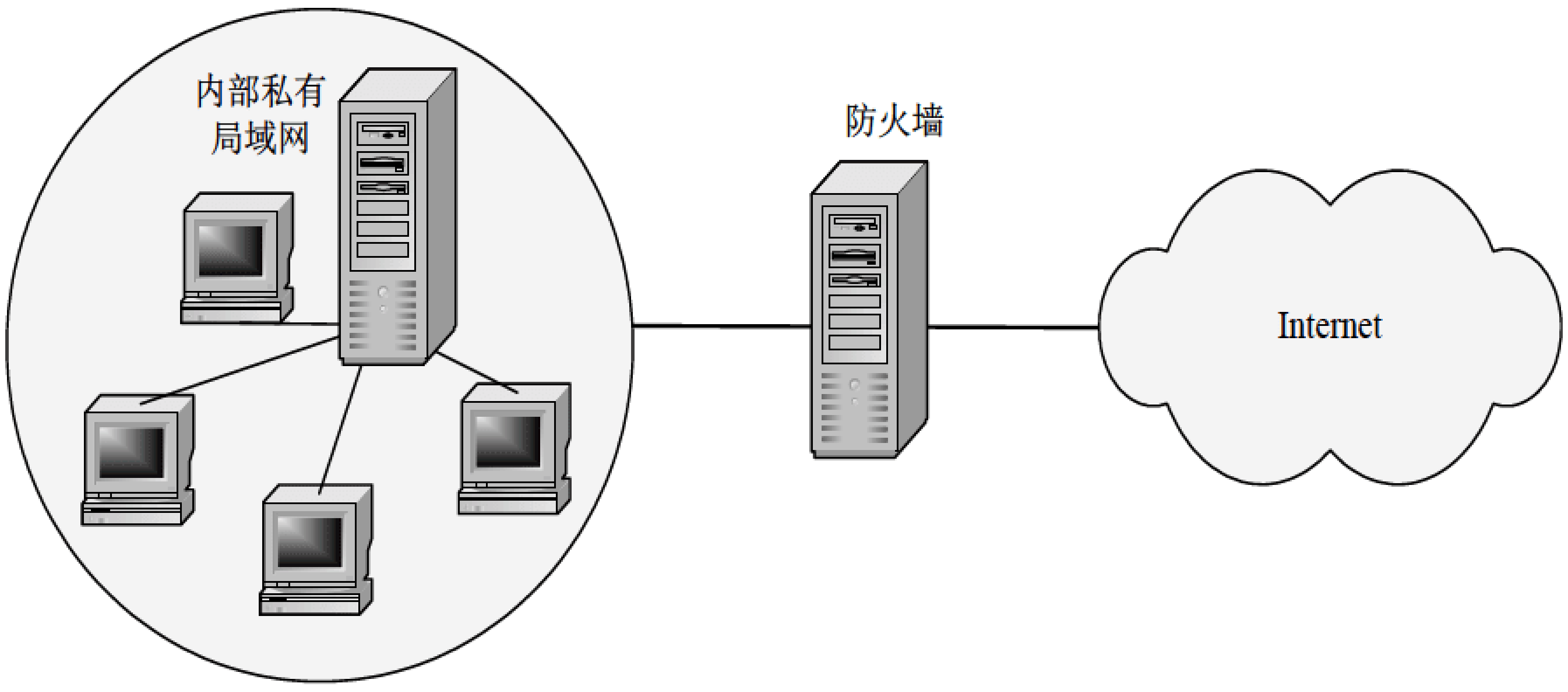


图 1-16　防火墙示意图

通过在网络中设置防火墙，可以过滤网络通信的数据包，对非法访问加以拒绝。系统设置防火墙后，可以为网络提供各种保护，主要包括以下几个方面的内容。

- 隔离不信任网段间的直接通信。
- 隔离网络内部不信任网段间的直接通信。
- 拒绝非法访问。
- 地址过滤。
- 访问发起位置的判断。
- 过滤网络服务请求。
- 系统认证。
- 日志功能。

利用防火墙技术，通常能够在内外网之间提供安全保护。但是，仅仅使用防火墙保证网络安全还远远不够，原因如下所述。

- 入侵者可寻找防火墙背后可能敞开的后门。网络结构的改变，有时会造成防火墙上的安全策略失效。
- 入侵者可能就在防火墙内。在每个企业的内部网络中，每个内部网段上除连接着

业务主机外，还有许多工作站，这些工作站与主机的通信不需要通过防火墙。如果攻击行为是从这些工作站上发起的，主机将处于无保护的状态。

◆ 由于性能的限制，防火墙不能提供实时的入侵检测能力。

单一应用防火墙技术，以上问题是不能得到有效解决的。如果公司在重要主机上安装实时入侵检测系统就可以解决由上述情况引起的安全问题。

3. 入侵检测系统

入侵检测系统(Intrusion Detection System，IDS)可以弥补防火墙的不足，为网络安全提供实时的入侵检测及采取相应的防护手段，如记录证据、跟踪入侵、恢复或断开网络连接等。

1) 基本概念

入侵行为主要是指对系统资源的非授权使用，可以造成系统数据的丢失和破坏、系统拒绝服务等危害。对于入侵检测而言的网络攻击可以分为以下 4 类。

(1) 检查单 IP 包(包括 TCP、UDP)首部即可发觉的攻击，如 winnuke、ping of death、land.c、部分 OS detection、source routing 等。

(2) 检查单 IP 包，并同时要检查数据段信息才能发觉的攻击，如利用 CGI 漏洞、缓存溢出攻击等。

(3) 通过检测发生频率才能发觉的攻击，如端口扫描、SYN Flood、smurf 攻击等。

(4) 利用分片进行的攻击，如 teadrop、nestea、jolt 等。

进行入侵检测的软件与硬件的组合就是入侵检测系统。入侵检测系统的原理模型如图 1-17 所示。入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

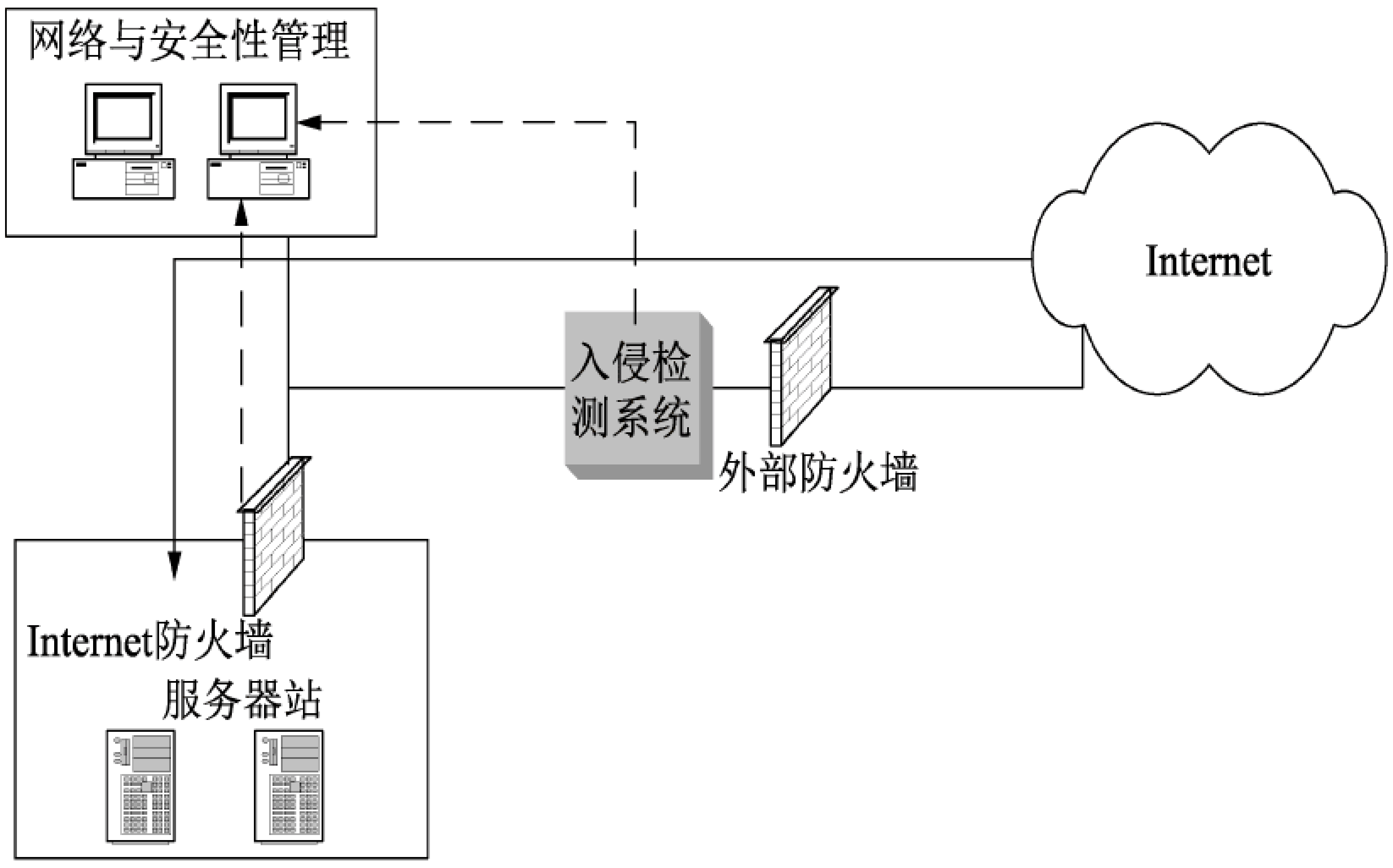


图 1-17 入侵检测系统的原理模型

2) 任务

入侵检测系统执行的主要任务包括监视、分析用户及系统活动；审计系统构造的弱点；识别、反映已知进攻的活动模式，向相关人士报警；统计分析异常行为模式；评估重要系统和数据文件的完整性；审计、跟踪管理操作系统，识别用户违反安全策略的行为。

3)　步骤

入侵检测一般分为 3 个步骤，依次为信息收集、数据分析、响应(被动响应和主动响应)。

信息收集的内容包括系统、网络、数据及用户活动的状态和行为。入侵检测利用的信息一般来自系统日志、目录以及文件中的异常改变、程序执行中的异常行为及物理形式的入侵信息 4 个方面。

数据分析是入侵检测的核心。它首先构建分析器，把收集到的信息经过预处理，建立一个行为分析引擎或模型，然后向模型中植入时间数据，在知识库中保存植入数据的模型。数据分析一般通过模式匹配、统计分析和完整性分析 3 种手段进行。

入侵检测系统在发现入侵后会及时做出响应，包括切断网络连接、记录事件和报警等。响应一般分为主动响应(阻止攻击或影响进而改变攻击的进程)和被动响应(报告和记录所检测出的问题)两种类型。

4)　入侵检测系统技术

可以采用概率统计方法、专家系统、神经网络、模式匹配、行为分析等来实现入侵检测系统的检测机制，以分析事件的审计记录，识别特定的模式，生成检测报告和最终的分析结果。

发现入侵检测一般采用如下两项技术。

(1)　异常发现技术。异常发现技术假定所有入侵行为都是与正常行为不同的。它的原理是，假设可以建立系统正常行为的轨迹，所有与正常轨迹不同的系统状态则视为可疑企图。异常阈值与特征的选择是其成败的关键。其局限在于：并非所有的入侵都表现为异常，而且系统的轨迹难以计算和更新。

(2)　模式发现技术。模式发现技术是假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征，所有已知的入侵方法都可以用匹配的方法发现。模式发现技术的关键是如何表达入侵的模式，以正确区分真正的入侵与正常行为。模式发现的优点是误报少；局限是只能发现已知的攻击，对未知的攻击无能为力。

5)　入侵检测系统的分类

通常，入侵检测系统按其输入数据的来源分为以下 3 类。

(1)　基于主机的入侵检测系统。其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

(2)　基于网络的入侵检测系统。其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

(3)　分布式入侵检测系统。能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，系统由多个部件组成，采用分布式结构。

另外，入侵检测系统还有其他一些分类方法。如根据布控物理位置可分为基于网络边界(防火墙、路由器)的监控系统、基于网络的流量监控系统以及基于主机的审计追踪监控系统；根据建模方法可分为基于异常检测的系统、基于行为检测的系统和基于分布式免疫的系统；根据时间分析可分为实时入侵检测系统和离线入侵检测系统。

6)　入侵检测的方法

入侵检测的方法主要有以下几种。

(1)　静态配置方法。静态配置方法通过检查系统的当前配置，诸如系统文件的内容或

者系统表，来检查系统是否已经或者可能会遭到破坏。静态是指检查系统的静态特征(系统配置信息)，而不是系统中的活动。所以，采用静态配置分析方法需要尽可能了解系统的缺陷，否则入侵者只需要简单地利用那些系统中未知的安全缺陷就可以避开检测系统。

(2) 异常性检测方法。异常性检测技术是一种在不需要操作系统及其防范安全性缺陷专门知识的情况下，就可以检测入侵者的方法，同时它也是检测冒充合法用户的入侵者的有效方法。但是，在许多环境中，为用户建立正常行为模式的特征轮廓，以及确定用户活动的异常性报警的阈值都是比较困难的事，所以仅使用异常性检测技术不可能检测出所有的入侵行为。

(3) 基于行为的检测方法。通过检测用户行为中那些与已知入侵行为模式类似的行为，以及那些利用系统的缺陷或间接违背系统安全规则的行为，来判断系统中的入侵活动。

入侵检测方法虽然能够在某些方面取得好的效果，但总体看来各有不足，因而越来越多的入侵检测系统都同时采用几种方法，以互补不足，共同完成检测任务。

7) 入侵检测系统的结构

目前，CIDF(通用入侵检测架构组织)和 IETF 都试图对入侵检测系统进行标准化。CIDF 阐述了一个入侵检测系统的通用模型，将入侵检测系统分为以下 4 个组件。

(1) 事件产生器。CIDF 将入侵检测系统需要分析的数据统称为事件，它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。事件产生器是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

(2) 事件分析器。事件分析器分析得到的数据，并产生分析结果。

(3) 响应单元。响应单元则是对分析结果做出反应的功能单元，它可以做出切断连接、改变文件属性等强烈反应，也可以是简单的报警。

(4) 事件数据库。事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

在这个模型中，前三者以程序的形式出现，而最后一个常是文件或数据流。入侵检测系统的几个组件常位于不同的主机上。一般会有 3 台机器，分别运行事件产生器、事件分析器和响应单元。

8) 入侵检测系统的标准化

IETF 的 Internet 草案工作组(IDWG)专门负责定义入侵检测系统组件之间，以及不同厂商的入侵检测系统之间的通信格式，目前只有相关的草案(Draft)，还未形成正式的 RFC 文档。IDWG 文档有以下 4 类。

(1) 入侵警报协议(IAP)。该协议是用于交换入侵警报信息、运行于 TCP 之上的应用层协议。

(2) 入侵检测交换协议(IDXP)。这个应用层协议是在入侵检测实体间交换数据，提供入侵检测报文交换格式(IDMEF)报文、无结构的文本和二进制数据的交换。

(3) IDMEF。IDMEF 是数据存放格式隧道(Tunnel)文件，允许块可扩展交换协议(Beep)对等体能作为一个应用层代理，用户通过防火墙得到服务。

(4) IAP。IAP 是最早设计的通信协议，它将被 IDXP 替换，IDXP 建立在 Beep 基础之上，Tunnel 文件配合 IDXP 使用。

9)　IDS 与防火墙的比较

IDS 不同于防火墙的是，它是一个监听设备，没有挂接在任何链路上，无须网络流量流经它便可以工作。因此，对 IDS 的部署，唯一的要求是：IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的 Hub 式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，IDS 在交换式网络中的位置一般选择在：尽可能靠近攻击源和受保护资源。这些位置通常是：服务器区域的交换机，Internet 接入路由器之后的第一台交换机，重点保护网段的局域网交换机等。两者的不同点如表 1-5 所示。

表 1-5　IDS 与防火墙功能的比较

比较项目	防 火 墙	IDS
设备类型	多穴主机，数据转发设备，完成类似于交换机和路由器的功能	一般为单接口，是数据采集、分析设备
流量处理机制	过滤	无
对受检报文的操作	大量读写各层报文首部	仅复制
对链路速度的影响	取决于转发延迟	无影响
可附加模块	可实现网络层加密、应用层病毒检测和杀毒功能	不能实现加密、杀毒功能，但可以实现病毒检测功能
对入侵行为的处理	拒绝、报警、日志记录	报警、日志记录和有限反击
入侵检测的准确性	基于流量转发负载压力，对报文普遍检查，可能发生误报、漏报	无转发负担，有入侵知识库支持，误漏报率较低
对访问日志的记录	只作条目式记录，框架较粗	非常详细，包括访问的资源和报文内容等
设备稳定性对网络的影响	要求非常高，否则可能造成网络链路的阻断	无
应用层内容恢复	一般不提供，但可据此进行过滤和替换功能	能够完整修复应用层内容，能够对网络特定流量进行全程监视和记录，为管理员判断进攻者、搜集证据提供了强有力的手段
对网络层以下各层的支持	由于对物理链路隔断，必须支持所有网络层以下的协议才能维持网络正常运作，如 RIP、OSPF、IGMP 等	不作要求

1.5.1.6　网络系统的评价

1. 系统评价概述

网络系统的评价也要遵循一般系统的评价原则，下面简要介绍系统评价的基本概念、价值、评价尺度、评价任务和评价步骤。

1) 系统评价的基本概念

所谓系统评价，是指根据预定的系统目的，在系统调查和可行性研究的基础上，主要从技术和经济等方面，就各种系统设计的方案所能满足需要的程度及消耗和占用的各种资源进行评审，选择技术上先进、经济上合理、实施上可行的最优或满意的方案。根据评价与系统的关系，可以区分出如表 1-6 所示的评价类型。

表 1-6 系统评价的类型

序 号	评价与系统的关系	评价的类型
1	评价与决策	决策前、中、后评价
2	评价与系统发展过程	事前、中、后评价
3	评价信息特征	基于数据、模型、专家知识的评价；综合评价

在系统开发过程中，通过系统工程的思想、程序和方法的应用，可以提出许多开发系统的可选方案，这时就要通过系统评价技术从众多的可选方案中找出最优的方案。然而，要决定哪一个方案最优却未必容易。

2) 价值

所谓价值，就是评价主体(个人或集体)对某个评价对象(如待开发的系统、待评价的方案等)的认识(主观感受)和估计。

价值是评价主体主观感受到的，是人们对客观存在的事物从各种各样的分析中主观抽象出来的。价值不是孤立地附属于某一评价对象，因此也就没有衡量价值的绝对尺度(标准)。

3) 评价尺度

系统评价是由评价对象、评价主体、评价目的、评价时期、评价地点等要素构成的一个综合性问题。因此，对评价技术来说，就是首先引进和确定评价尺度(标准)，然后利用评价尺度对评价对象进行测定，并确定其价值。

常用的评价尺度大致可分为 4 种。第一种称为绝对尺度，即规定原点尺度不变。第二种称为间隔尺度，有些场合只要测得数值差就有意义。第三种是顺序尺度，它可以用顺序或反映顺序的字符来表示，这时需要的只是其顺序关系。最后一种是名义尺度，这仅仅是为了识别或分类需要而用数字与对象相对应。如学校的班级编号和运动员的编号等就是这种名义尺度。

在评价中，要根据评价的目的和评价对象的性质来确定评价尺度。

4) 系统评价的任务

系统评价的主要任务就在于从评价主体根据具体情况所给定的、可能是模糊的评价尺度出发，进行首尾一致的、无矛盾的价值测定，以获得对多数人来说均可以接受的评价结果，为正确决策提供所需的信息。由此可见，系统评价和决策是密切相关的。为了在众多替代方案中做出正确的选择，就需要有足够丰富的信息，其中包括足够的评价信息。所以说，系统评价只有和方案决策和行为决策联系起来才有意义。评价是为了决策，而决策需要评价，决策过程需要评价过程。

5) 系统评价的步骤和构成

如图 1-18 所示，系统评价的一般步骤包括评价问题、评价系统分析(前提条件探讨)、

评价资料的搜集、评价指标的选择、评价函数的确定、评价价值的计算和综合评价等几个阶段。

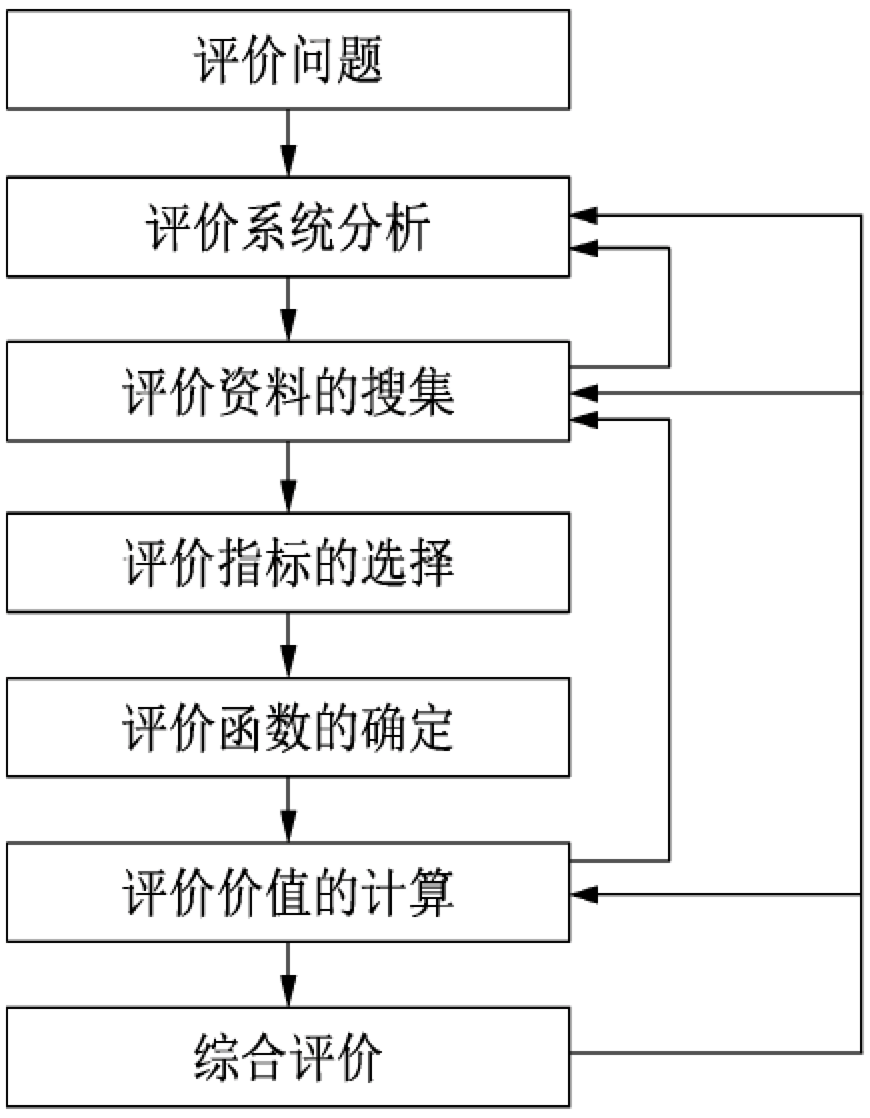


图 1-18　系统评价步骤

2. 系统评价要点

系统评价的要点包括评价系统分析、评价资料的搜集、评价指标的选择、评价函数的确定、评价价值的计算和综合评价等。

1)　评价系统分析

在正式进行系统评价前，有必要对评价系统进行分析，探讨和明确一系列前提条件，这是做好系统评价的首要工作。主要包括如下内容。

(1)　评价的目的。总体来说，评价的目的是为了更好地决策，但具体来说，评价目的又大致可分为以下 4 个方面。

①　使评价系统达到最优。为了使系统结构或技术参数达到最优，有必要量化评价系统中各种替代方法的价值。

②　对决策的支持。当评价者或决策者在选择最优方案的过程中，对替代方案的各自价值感到迷惑不解时，评价提供的信息可供决策参考。

③　决定行为的说明。对于复杂的问题即使做出合理的决定，如果没有评价或评价过程模糊不清，也会遭到人们的怀疑、误解以至抵制，所以为了形成统一意志，需要有某种程度的客观评价。

④　问题的分析。评价的过程往往是问题分析的过程。有许多问题利用相关的评价方法可以把复杂的问题分解成简单的小问题，再通过对这些小问题的分析和评价，获得系统的综合评价。

(2)　评价系统范围的界定。它主要是确定系统的边界，即评价对象涉及多大范围。评价系统的范围不应过小，以免忽略重要影响部门而有失系统性；同时也不应过大，以免使评价问题过度复杂化。

(3)　评价的立场。在进行系统评价时必须明确评价主体的立场，即明确评价主体是系统使用者还是开发者抑或是第三者等，这对于以后评价方案的确定、评价项目的选择等都

有直接的影响。

(4) 评价的时期。即系统评价处于系统开发全过程的哪个时期(评价时期一般可分为事前评价、事中评价和事后评价)。

(5) 评价系统环境的分析。系统环境的分析是指对存在于系统外的物质的、经济的、信息的影响因素进行分析，以了解这些因素对评价系统的影响。系统环境可能受到的影响可分为三大类：技术的、经济的及社会的影响。

2) 评价资料的搜集

对评价系统的功能、费用、时间及其使用寿命进行预测和估计，为确定评价尺度、评价函数等搜集评价所需的资料。

3) 评价指标的选择

评价指标的选择是由评价目标与实际情况共同决定的，选择时应注意以下几点。

(1) 评价指标必须与评价目的和目标密切相关。

(2) 评价指标应当构成一个完整的体系，即全面地反映所需评价对象的各个方面。

(3) 评价指标总数应当尽可能地少，以降低评价负担。

4) 评价函数的确定

评价函数是使评价定量化的一种数学模型。不同问题使用的评价函数可能不同，同一个评价问题也可以使用不同的评价函数，因此，对选用什么样的评价函数本身也必须做出评价。一般应选用能更好地达到评价目的的评价函数或其他适应的评价函数。

评价函数本身是多属性、多目标的。尤其当评价目的在形成统一意见或进行群体决策时，对确定评价函数会产生不同的看法。因此，在系统实施进行之前，应该在有关人员间进行充分的无拘束的讨论，否则难以获得有效的评价。

5) 评价价值的计算

当评价函数确定后，评价尺度也随之确定。在评价价值计算之前，还需要确定各评价项目的权重。总之，评价尺度和评价项目的权重应保证评价的客观正确性和有效性。

6) 综合评价

综合评价就是对系统进行技术、经济、社会等各方面的全面评价。但综合评价的各个方面和评价项目不能一概而论，应根据具体评价对象确定。以企业开发新产品为例，一个完整的综合评价体系大致包括以下几个方面：经营管理方面、技术方面、市场方面、时间方面、经济方面、体制方面和社会方面等。

安排定期的系统评价被确定为网络系统实施过程实现后鉴定的一部分。定期的系统评价安排在系统实现后 3 个月，但不能超过一年。评价小组负责审定下列内容。

- 系统效率。
- 系统有效性。
- 解决周期。
- 响应时间。
- 信息的关联。
- 输入/输出的分配及控制。
- 输入/输出的格式和内容。

- 文件、记录和数据库的结构。
- 更新和后备措施。
- 系统资料的通用性。

关于需要进一步改进的不足之处和建议都要编制成文件，并提交给相应业务领域的管理人员。

3. 系统能力的限制

网络系统的主要功能是资源共享和数据传输，因而系统的能力具体体现在服务器处理能力和传输能力，即媒体的带宽和中继设备的交换能力。由于每种设备的配置是固定的，因而其处理能力也有一定的范围限制，若传输媒体带宽固定，其单位时间内的传输能力也有一定的限制，则还要考虑利用率的问题。因此在系统评价时应该确切地了解系统的设备配置及其性能，对即将开放的网络服务进行评估，考查是否超出网络系统的能力，如果不能满足则不应该接受，采取其他措施扩容或者限制网络用户的应用，以保证网络系统正常可靠地运行。

4. 潜在的问题分析

系统设计实施完成后，需要对整个系统进行评估，即要考查系统的功能、性能、可靠性、可用性、安全性等方面是否达到设计目标，需要分析各个方面是否存在潜在的问题隐患，为网络系统的维护和升级提供依据。

1)　网络性能问题分析

使用多种性能监视工具对包括带宽、利用率、吞吐量、系统延时等在内的关键性能指标进行监控并记录结果，与基准线进行比较，观测系统性能出现波动的时间和周期并分析其原因。

2)　网络安全性问题分析

可从以下方面对网络安全性问题进行分析。

(1)　从网络系统外部进行分析，考查计算机网络基础设施中防火墙的安全性。

(2)　从网络系统内部进行分析，考查网络系统内部计算机的安全性。

(3)　从网络应用系统进行分析，考查每台硬件设备运行的操作系统的安全性。

(4)　使用专用软件进行分析，查找存在的安全漏洞和隐患并提出解决方案。

3)　网络可靠性问题分析

与有关专家一道全面分析网络的可靠性，包括物理方面、逻辑方面的可靠性及其健康运行性，评估系统与需求的相合性，如果不相合则存在差距。还应该考虑到网络系统运营后新的应用需求及其增长所带来的影响，预期未来几年内网络可靠性存在的问题，并写入评估报告。

4)　形成问题报告

网络系统分析人员整理已经收集完整的各方面的评估报告，进一步分析找出系统存在的各方面问题，形成全面的问题报告。问题报告中应该详细描述问题存在的原因、发生的相关环境及对应用可能存在的影响，并将其提交给上一层决策者，作为系统升级时的参考依据。

1.5.1.7 改进系统的建议

1. 系统生命周期

开发一个新的网络系统或修改一个已有的网络系统的过程称为网络的生命周期。网络的生命周期体现的是一个新的网络或新特征的构思计划、分析设计、实施运行和维护的过程，这个过程在修改之后又要重新开始。这种生命周期与软件工程中的软件的生命周期非常类似。

虽然目前没有哪个生命周期可以完美地描述所有的项目开发，但是网络流程周期和网络循环周期这两种基本的生命周期模型得到了软件工程师的认可和应用。下面针对这两种网络生命周期进行介绍。

1) 网络流程周期

网络流程周期由需求规范、通信规范、逻辑网络设计、物理网络设计和实施阶段等 5 个不同的阶段组成。生命周期又叫作一个流程，因为每一项工作都是从一个阶段“流到”下一个阶段，正如图 1-19 所描绘的那样。当系统正常运行以后，网络生命周期就会由于更新而重新开始。

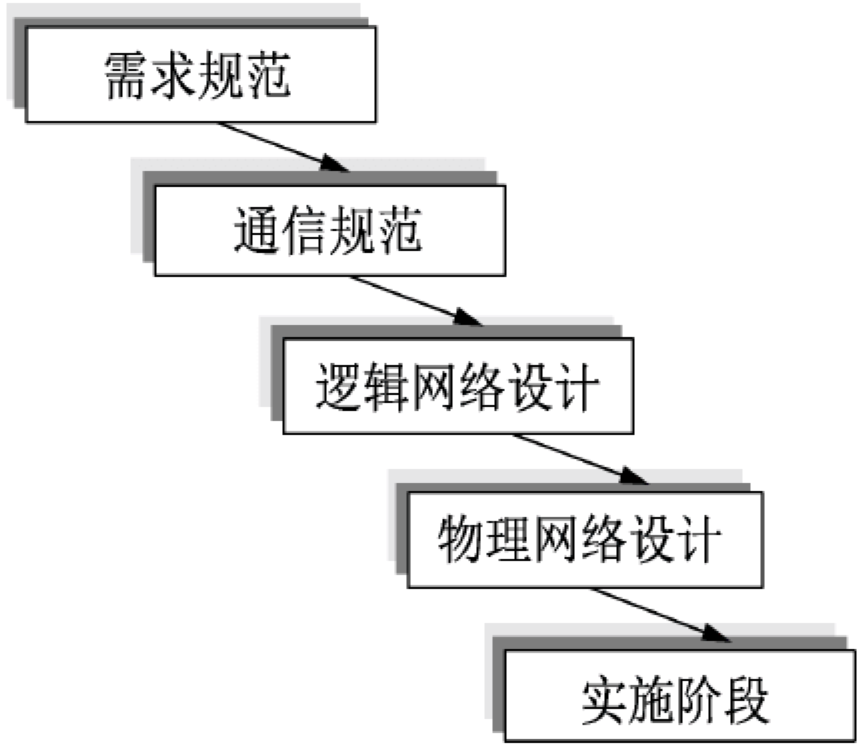


图 1-19 网络流程周期

按照这种模型开发网络，在开始下一个阶段之前，前面的每个阶段的工作必须已经完成。一般情况下，不允许返回前面的阶段，如果前一阶段的工作没有完成就进入了下一个阶段，则会造成工期拖延，随之将带来严重的超支。

网络流程周期的主要优势在于所有的计划都在较早的阶段完成。该系统的所有负责人对系统的具体情况以及工作进度都非常清楚，这就有助于较早地知道工期和更容易地协调工作。

网络流程周期的缺点是比较呆板、不灵活。因为在项目完成之前，用户的需求往往会发生变化，这使得已开发的部分需要经常修改，从而影响工作的进程。网络流程周期适用于开发很小的项目。

2) 网络循环周期

网络循环周期又称为网络旋涡周期，是从网络流程周期演变而来的。其出现的目的是克服网络流程周期在灵活性方面的缺点。

变化管理是网络循环周期的指导性原则。与网络流程周期不同的是，网络循环周期能够快速适应新的需求。这可以通过重复几次所有阶段来实现，每次循环将产生一个新的循

环周期。网络循环周期共由 4 个阶段组成，其各阶段的组成顺序如图 1-20 所示。

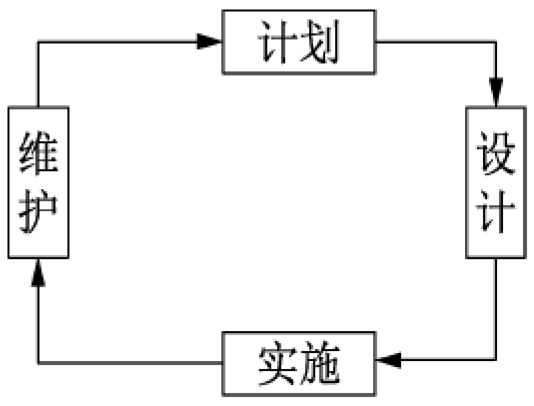


图 1-20　网络循环周期

网络循环周期是一个连续体，通过在网络设计中的每一个循环实现最终性能的一个子集，用户就有机会在项目完成之前反馈他们的意见和建议并在新的一轮循环中加以考虑，新的性能被加入，用户提出的问题随之得以解决。

虽然网络循环周期在处理需求变化方面比网络流程周期优越，但也有其自身的缺点，就是无法预知用户以后会要求什么，这样就很难估计出最终的经费和完工日期。最糟的是，按照网络循环周期模型开发网络，很容易陷入无休止的更新循环中。

2. 系统经济效益

付出应当有所得，而且应当大大地超出付出，这是市场经济的基本原则。因此，网络系统评价的另一个重点是投资/效益分析。投资分析参见技术可行性的结果；效益分析包括经济效益和社会效益两部分。经济效益又可进一步划分为直接经济效益和间接经济效益两部分。

直接经济效益是指通过本项工程的实施所产生的可见的经济效益，例如，使用自动化处理和电子化传输技术可以节省日常的邮政费用、差旅费开支等。

间接经济效益是指通过本项工程的实施所产生的间接经济效益，例如，节省人力、提高自动化程度、提高功效及加快部门内或者部门间的信息交互等。

对于经济效益分析，应当尽可能地考虑各个方面，并进行量化，包括节省了多少时间、节省了多少人力和工作量，相当于创造多少产值。例如，使用办公自动化，减少了人工录入的工作，不仅节省了人力，还降低了录入的差错，以及避免由此而引起的问题。

需要指出的是，在分析投资/效益比时，也应当对投资风险进行分析。事实上，进行任何投资活动时，必然存在着某种风险。一味地描述效益而忽略可能的风险是不明智的。投资风险主要体现在如下几个方面：实际投资值超过估计值；应用效果比预期的差；效益比预期的低；出现不可预测的意外或环境变化。在进行可行性分析时，应当考虑各种投资风险的可能性，并提出降低风险的措施，亦即可行性分析应当客观地反映所有的问题。

3. 系统的可扩充性

可扩充性是满足所有网络通信流量的需求并随着公司的发展能够容纳更多通信流量的一种能力。可扩充性涉及网络设计的几个方面。如以校园网为例，需要考虑以下几个方面。

- 计算机工作站将要用到的重要的服务器资源放在何处。
- 使用的网络技术能否支持放置在每个楼层的所有工作站。
- 连接校园网的主干网能否支持全校所有的工作站间的跨建筑通信量。
- 集线器和交换机是否有足够的带宽能力处理各楼层和建筑物间的通信量。
- 网络协议是否能够正确地对环境里的每台工作站进行寻址。

◆ 局域网环境能否容纳广播站的容量。
◆ 网络内两个最远节点间的距离是否超出了所用网络技术允许的范围。
◆ 网络是否存在要求特别高的工作组，对它们应如何处理。

可扩充性是在网络规划设计阶段就应该考虑的问题，在网络设计中，应该保留一定的扩展空间，以备以后网络升级之用。但随着系统的运行和升级，可扩展性将逐步丧失，因此在网络系统升级时也应该考虑这个问题，以便长久地保持系统可扩充的能力。

4. 建议改进系统的要点

网络系统正常运行后，经过网络管理人员长时间对系统性能、安全、可靠性、可用性、可扩充性等方面的观察和数据积累，系统出现的问题会越来越清晰地显示在面前。如：

◆ 安全漏洞和安全隐患。
◆ 性能瓶颈。
◆ 可靠性措施不力。
◆ 可用性不符合需求。
◆ 扩充空间有限，不能满足今后应用。

根据对系统存在问题的分析并参照潜在问题分析的报告，可以针对每个问题进行改进，以使整个网络更加安全可靠地运行。

1.5.2 典型例题分析

例 1 【说明】(2017 年下半年下午试题一)

图 1-21 是某企业网络拓扑，网络区域分为办公区域、服务器区域和数据区域，线上商城系统为公司提供产品在线销售服务。公司网络保障部负责员工办公电脑和线上商城的技术支持和保障工作。

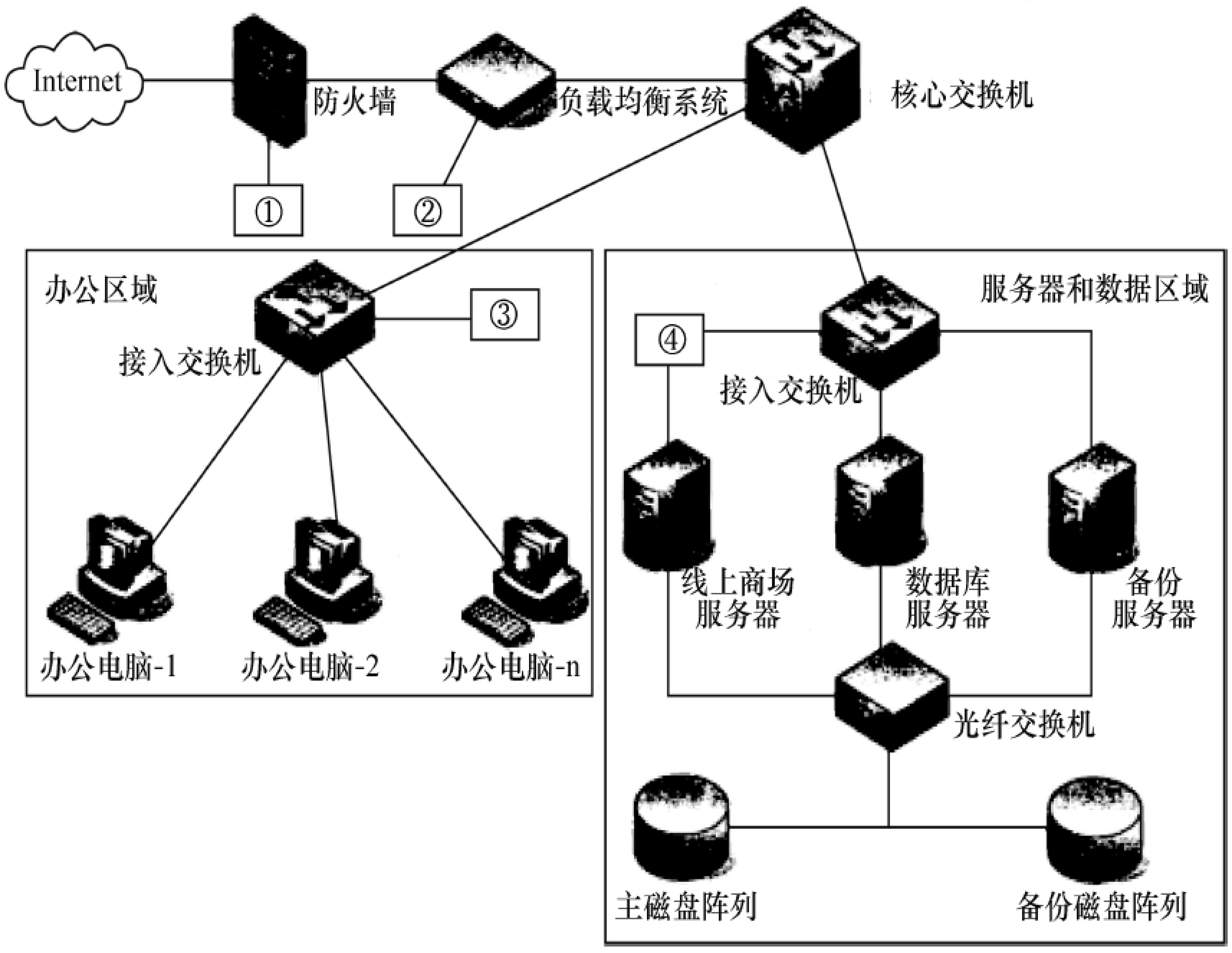


图 1-21 某企业网络拓扑

【问题 1】(6 分)

某天，公司有一台电脑感染“勒索”病毒，网络管理员应采取__(1)__、__(2)__、__(3)__措施。

(1)～(3)备选答案：

A. 断开已感染主机的网络连接

B. 更改被感染文件的扩展名

C. 为其他电脑升级系统漏洞补丁

D. 网络层禁止 135/137/139/445 端口的 TCP 连接

E. 删除已感染病毒的文件

【问题 2】(8 分)

图 1-21 中，为提高线上商城的并发能力，公司计划增加两台服务器，三台服务器同时对外提供服务，通过在图中__(4)__设备上执行__(5)__策略，可以将外部用户的访问负载平均分配到三台服务器上。

(5) 备选答案：

A. 散列　　B. 轮询　　C. 最少连接　　D. 工作一备份

其中一台服务器的 IP 地址为 192.168.20.5/27，请将配置代码补充完整。

ifcfg-eml 配置片段如下：

```
DEVICE =eml
TYPE=Ethernet
UUID=36878246-2a99-43b4-81df-2db1228eea4b
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
HWADDR=90:B1:1C:51:F8:25
IPADDR=192.168.20.5
NETMASK=__(6)__
GATEWAY=192.168.20.30
DEFROUTE= yes
IPV4_FAILURE_FATAL=yes
IPV6INTI=no
```

配置完成后，执行 systemct1__(7)__network 命令重启服务。

【问题 3】(4 分)

网络管理员发现线上商城系统总是受到 SQL 注入、跨站脚本等攻击，公司计划购置__(8)__设备/系统，加强防范；该设备应部署在图 1-21 中设备①～④的__(9)__处。

(8)备选答案：

A. 杀毒软件　　B. 主机加固　　C. WAF(Web 应用防护系统)　　D. 漏洞扫描

【问题 4】(2 分)

图 1-21 中，存储域网络采用的是__(10)__网络。

答案：

【问题1】(1) A　(2) C　(3) D

【问题2】(4) 负载均衡系统　(5) B　(6) 255.255.255.224　(7) restart

【问题3】(8) C　(9) ④

【问题4】(10) FC-SAN

解析：

【问题1】勒索病毒利用的是Windows系统漏洞，通过系统默认开发135、137、139、445等文件共享端口发起的病毒攻击，因此应该先将感染的主机断开网络连接，将其他主机也断开连接，并禁止共享操作，然后升级操作系统漏洞补丁，避免再次遭受攻击。

【问题2】实现负载均衡可直接在此网络上的负载均衡设备实现，并执行轮询设置，这样可实现对各服务器的负载均衡操作。由题可知服务器的IP地址为192.168.20.5/27，因此可知子网掩码为255.255.255.244，重启服务器的命令为systemctl restart network。

【问题3】Web应用防护系统，简称WAF。Web应用防火墙是执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一种产品。它能够有效发现及阻止SQL注入，网页篡改，跨站脚本等攻击。其主要对服务器区域进行检测和保护，故放入④处最为适宜。

【问题4】存储网络，采用光纤连接存储区域，实现高速存储访问，符合FC-SAN支持块级调用，适合为大型数据库提供存储服务。

例2　阅读以下说明，回答问题1～2，将解答填入答题纸对应的解答栏内。

【说明】

网络解决方案如图1-22所示。该网络原先使用的是国外品牌的交换机，随着网络规模的扩大，增添了部分国产品牌的交换机，交换机1至交换机5均是国产10～100 Mb/s的自适应交换机，交换机6和交换机7是第三层交换机。

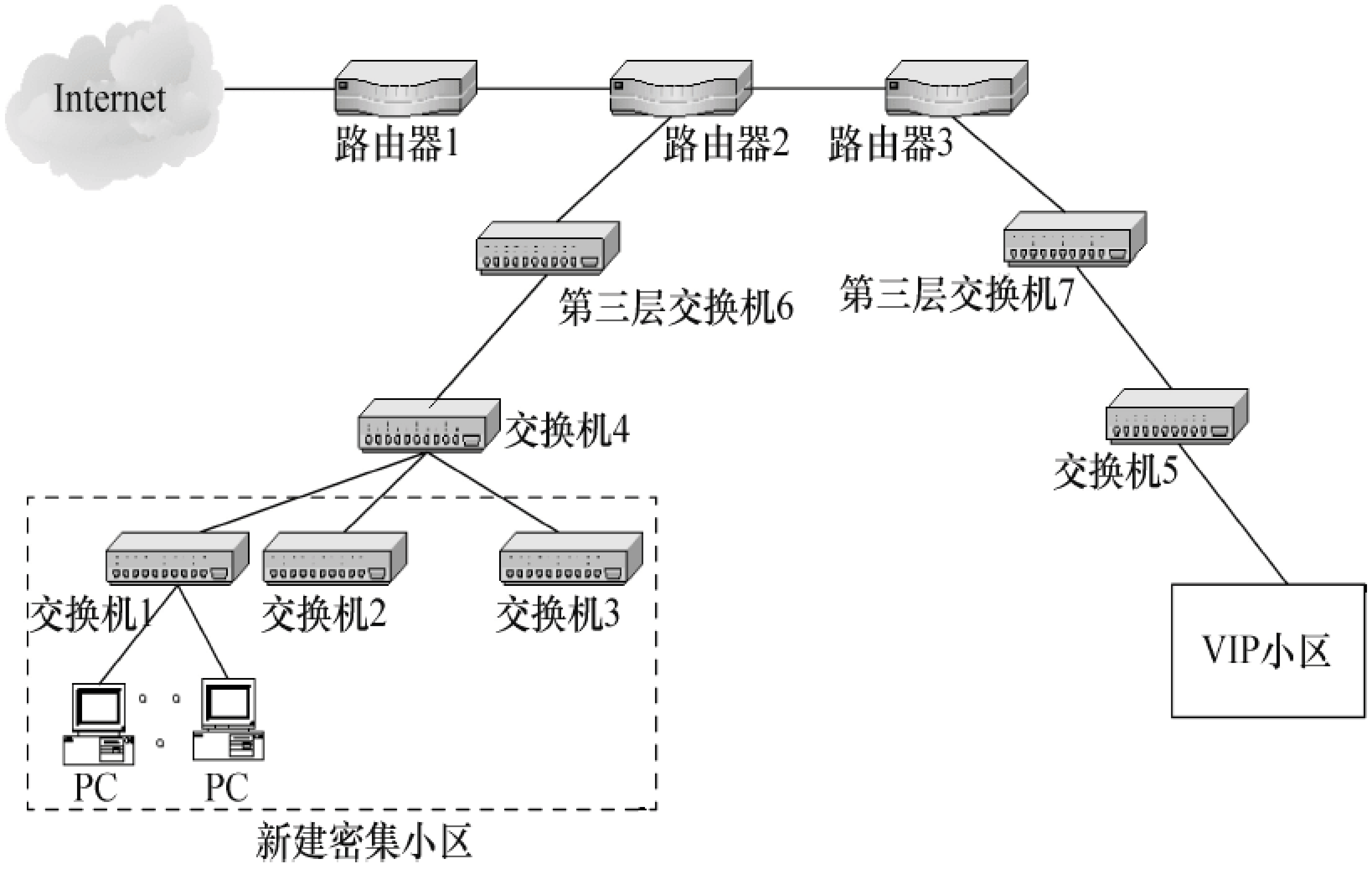


图1-22　网络解决方案

该网络在运营过程中曾出现下列故障。

故障1

使用“网络故障一点通”测试新建密集小区用户和第三层交换机6之间的最大吞吐量，

发现这些用户带宽都不超过 10 Mbps。

使用“在线型网络万用表”串联在第三层交换机 6 和交换机 4 之间，测试数秒钟后，发现它们之间的传输速率也是 10 Mb/s。

故障 2

故障现象：VIP 小区的用户不能上网，但能 ping 通路由器地址。

分析：由于 VIP 小区的用户配置的是静态 IP 地址，而且处在同一网段，共用路由器上的一个地址作为网关地址。用户能 ping 通路由器，说明从用户到路由器间的路径是通的，因此需重点检查路由器。

操作过程如下。

首先，在路由器上，观察接口状态，未见异常。

然后，用 show ip route 观察__①__表，未见异常。

最后，再用 show arp 观察__②__表，发现路由器的 MAC 地址与工作人员以前保存在该表中的 MAC 地址不同，而是 VIP 小区中某个用户的 MAC 地址。

【问题 1】造成故障 1 的原因是什么？如何解决？

【问题 2】

(1)　将故障 2 中①和②两处合适的答案填入答题纸相应的解答栏内。

(2)　故障 2 如何解决?

答案：

【问题 1】交换机 6 的端口是 10 Mbps 端口，可以升级为 100 Mbps 端口。

【问题 2】

(1)　①IP 路由　②ARP

(2)　重新修改 ARP 表中的路由器的 MAC 地址。

解析：根据测试结果可知交换机 4 和交换机 6 之间的带宽为 10 Mbps，而由于交换机 1 和交换机 4 都是自适应交换机，因而可以判断第三层交换机 6 的端口带宽最高为 10 Mbps，故解决此问题的简单方法就是将交换机 6 的端口升级，比如升级为 100 Mbps 的端口，这样可以提升 PC 的访问速率。

对于第 2 个故障，关键在于了解访问互联网的过程。在网络中存在多种标识主机的方法，包括域名、IP 地址和 MAC 地址，对于同一台主机来说，它们应该是一致的，即具有一一对应的关系。而其中 MAC 地址是网络接口卡的物理地址，可以唯一确定一台主机，其他名称均可以改变。本题的故障在于 IP 地址与 MAC 地址的对应关系弄错了，因而无法找到正确的路由器接入互联网。解决的办法是修改 ARP 表中路由器 1 对应的 IP 地址与 MAC 地址的对应关系。

另外，还需要掌握查看故障时常用的 show 命令的用法。

例 3　公司网络中的设备或系统(包括存储商业机密的数据库服务器、邮件服务器、存储资源代码的 PC、应用网关、存储私人信息的 PC、电子商务系统)哪些应放在 DMZ 中，哪些应放在内网中？并给予简要说明。

答案：在 DMZ 中放置邮件服务器、应用网关、电子商务系统。在内网中放置机密数据库服务器、存储私人信息的 PC 和存储资源代码的 PC。DMZ 是放置公共信息的最佳位置，

用户、潜在用户和外部访问者不用通过内网就可以直接获得他们所需的关于公司的一些信息。公司中机密的、私人的信息可以安全地存放入内网中，即 DMZ 的后面。DMZ 中的服务器不应包含任何商业机密、资源代码或私人信息。

解析：当打算在网络上安装一个防火墙时，首先想到的可能就是把所有的客户和服务器都放到它的后面。这对于小企业来说是一个较好的解决办法，但对于大企业，就应该考虑构建一个叫作非军事区 DMZ(Demilitarized Zone)的周边安全网络，用来区分外网与内网。

DMZ 是放置公共信息的最佳位置，这样用户、潜在用户和外部访问者都可以直接获得他们所需的关于公司的一些信息，而不用通过内网。公司中机密的和私人的信息可以安全地存放在内网中，即 DMZ 的后面。DMZ 中的服务器不应包含任何商业机密、资源代码或是私人信息。DMZ 服务器上的破坏最多只可能造成在恢复服务器时的一段中断服务。

1.5.3　同步练习

1. 试述一般连接性故障排除的步骤。
2. 在两个公司网站之间建立一条租用(DDN)线路连接时遇到以下问题。

过去这两个网站是通过 ISDN 线路使用 DDR 来连接的，由于信息量的增加，选用 256 Kb/s 的租用线路更加合算。连接方式如图 1-23 所示。

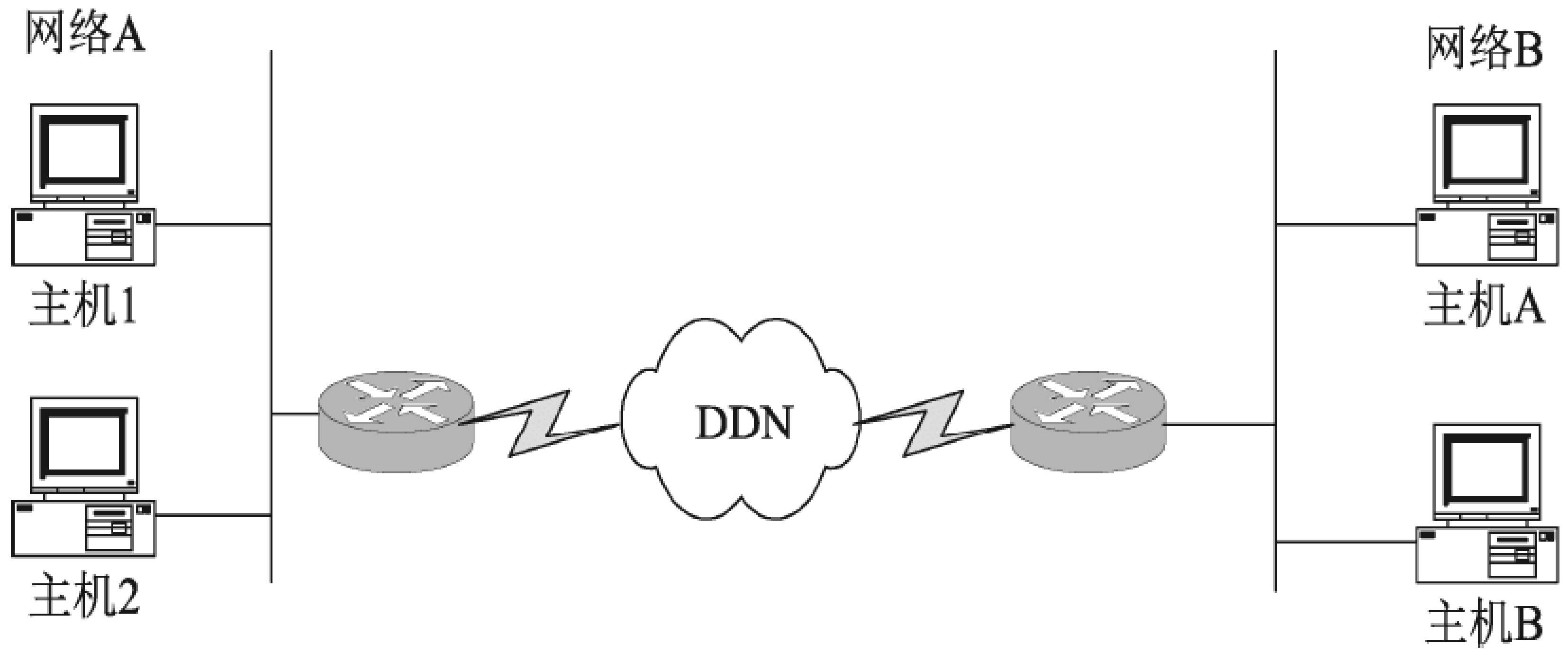


图 1-23　线路连接方式

现在决定为每个路由器配一个 NAN 串口网卡，提供 DB-60 串口，以便连接到电话公司的网络终端(NTU)上。电话公司派人到两个网站进行了实地观察，并且安装了 NTU。先将两个网站的路由器的 DB-60 与 V.35 电缆相连接，然后开始进行路由的配置。建立这个配置后，两个路由器上的串口都不能运行，它们显示为无法工作的状态。

(1)　如果假定最初的配置有问题，那么用什么命令可以检查?

(2)　检查完配置后发现并没有问题，然后决定按照 OSI 模型的顺序来进行系统的问题诊断。首先观察路由器的物理接口和 NTU，那么可以根据 NTU 的指示灯的哪个状态来判断它是正常的?

(3)　判断 NTU 正常后，如果想查看连接到路由器上的 DB-60 串口的电缆的状态，则哪个命令可以查看这个状态?

(4)　路由器与 DB-60 串口连接电缆的状态如下所示，根据这两个输出找出问题所在。

```
HD unit 0,idb=0x96138,driver structure at 0x9A600
```

```
Buffer size 1524 HD unit 0,V.35 DCE cable
Cpb=0x21,eda =0x4940,cda=0x4800
RX ring with 16 entries at 0x214800
...
```

1.5.4　同步练习参考答案

1. **答案：**

从近到远逐一检查与连接有关的设备，确定故障位置，然后排除故障。

连接性故障可能发生在 OSI 七层中的任何一个层次，在得到确认前，不要假定连接性的任何一个方面或者任何配置是正确无误的。其具体的步骤如下。

步骤 1：检查客户机和服务器上的 TCP/IP 地址和默认网关。可使用 ipconfig/all 命令。

步骤 2：确定客户机或服务器是否可以 ping 通它们的默认网关。

步骤 3：确认客户机是否可以 ping 通服务器的 TCP/IP 地址和主机名。

步骤 4：如果用 IP 地址可以 ping 通但用主机名却 ping 不通，则可能是名称解析问题。

步骤 5：如果客户能 ping 通服务器，但无法和应用建立连接，则可能是应用服务未启用。

2. **答案：**

(1)　应当用 show running-config 命令查看当前路由器的配置文件。

(2)　NTU 的灯应当是绿色的。

(3)　show controllers。

(4)　在这两个输出中，电缆显示的状态都是 V.35 DCE，而这里需要的是 V.35 DTE 电缆。将它们修改成 DTE 电缆后，串口将立即恢复为 Interface Up、Protocol Up 状态，这时就能够使两个网站之间的线路进行通信了。

1.6　本 章 小 结

本章知识点在 2014 年的新大纲中变化较小，只是一些表述方式的调整。

本章主要介绍了网络规划设计中的主要阶段，包括网络需求分析、网络设计、网络的构建和测试、网络的运行和维护以及网络系统的管理和评价。

本章内容在网络规划和设计中是很重要的一部分，也是大纲中要求重点掌握的内容。不过，从最近 5 年的考试来看，直接涉及的知识点不多，然而在往年的题目中，偶尔也会间接考查到。所以，在本书中把这部分内容压缩为一章，供读者复习时参考，希望考生灵活掌握。

第 2 章　交换机配置与 VLAN

大纲要求：

◆ 交换机的配置，包括命令行接口配置、Web 方式访问交换机。

◆ VLAN 配置。

◆ 多层交换机功能和机制。

2.1　交换机的基本配置

2.1.1　考点辅导

2.1.1.1　交换机的特性

局域网交换机拥有许多端口，每个端口都有自己的专用带宽，并且可以连接不同的网段。交换机各个端口之间的通信是同时的、并行的，这就大大提高了信息吞吐量。为了进一步提高性能，每个端口还可以只连接一个设备。

为了实现交换机之间的互联或与高档服务器的连接，局域网交换机一般拥有一个或几个高速端口，如 100Mbps 以太网端口、FDDI 端口或 155Mbps ATM 端口，从而保证整个网络的传输性能。

通过集线器共享局域网的用户不仅是共享带宽，而且是竞争带宽。可能由于个别用户需要更多的带宽而导致其他用户的可用带宽相对减少，甚至被迫等待，因而也就耽误了通信和信息处理。利用交换机的网络微分段技术，可以将一个大型的共享式局域网的用户分成许多独立的网段，减少竞争带宽的用户数量，增加每个用户的可用带宽，从而缓解共享网络的拥挤状况。由于交换机可以将信息迅速而直接地送到目的地，能大大提高速度和带宽，能保护用户以前在介质方面的投资，并能提供良好的可扩展性，因此交换机不但是网桥的理想替代物，而且是集线器的理想替代物。

与网桥和集线器相比，交换机从以下方面改进了性能。

◆ 通过支持并行通信，提高了交换机的信息吞吐量。

◆ 将传统的一个大局域网上的用户分成若干工作组，每个端口连接一台设备或连接一个工作组，可有效地解决拥挤现象。人们称这种方法为网络微分段(Micro-segmentation)技术。

◆ 虚拟网(Virtual LAN)技术的出现，给交换机的使用和管理带来了更大的灵活性。我们将在后面专门介绍虚拟网。

◆ 端口密度可以与集线器相媲美，一般的网络系统都有一个或几个服务器，而绝大部分都是普通的客户机。客户机都需要访问服务器，这样就导致服务器的通信和事务处理能力成为整个网络性能好坏的关键。

交换机主要是从提高连接服务器的端口的速率以及相应的帧缓冲区的大小，来提高整个网络的性能，从而满足用户的要求。一些高档的交换机还采用全双工技术进一步提高端口的带宽。以前的网络设备基本上都是采用半双工的工作方式，即当一台主机发送数据包的时候，它就不能接收数据包，当接收数据包的时候，就不能发送数据包。由于采用全双工技术，即主机在发送数据包的同时，还可以接收数据包，普通的 10 Mbps 的端口就可以变成 20 Mbps 的端口，普通的 100 Mbps 的端口就可以变成 200 Mbps 的端口，这样就进一步提高了信息吞吐量。

2.1.1.2　交换机的工作原理

传统的交换机本质上是具有流量控制能力的多端口网桥，即传统的(二层)交换机。把路由技术引入交换机，可以完成网络层的路由选择，故称为三层交换，这是交换机的新进展。交换机(二层交换)的工作原理和网桥一样，是工作在链路层的联网设备，它的各个端口都具有桥接功能，每个端口可以连接一个 LAN 或一台高性能网站或服务器，能够通过自学习来了解每个端口的设备的连接情况。所有端口由专用处理器进行控制，并经过控制管理总线转发信息。

同时可以用专门的网管软件进行集中管理。除此之外，交换机为了提高数据交换的速度和效率，一般支持多种方式。

1. *存储转发*

所有常规网桥都使用存储转发方法。它们在将数据帧发往其他端口之前，要把收到的帧完全存储在内部的存储器中，对其检验后再发往其他端口，这样其延时等于接收一个完整的数据帧的时间及处理时间的总和。如果级联很长时，会导致严重的性能问题，但这种方法可以过滤掉错误的数据帧。

2. *直通转发法*

直通转发法只检验数据帧的目标地址，这使得数据帧几乎马上就可以传出去，从而大大降低延时。其缺点是：错误帧也会被传出去。在错误帧的概率较小的情况下，可以采用切入法以提高传输速度。而在错误帧的概率较大的情况下，可以采用存储转发法以减少错误帧的重传。

2.1.1.3　交换机的配置

下面以华为公司的 S5700 系列交换机为例，介绍交换机的一般配置过程。

1. *电缆连接及终端配置*

如图 2-1 所示，接好 PC 机和交换机各自的电源线，在关机状态下，把 PC 机的串口 1(COM1)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。

图 2-1　仿真终端与交换机的连接

交换机 Console 端口的默认参数如下。

- ◆ 端口速率：9600bps。
- ◆ 数据位：8。
- ◆ 奇偶校验码：无。
- ◆ 停止位：1。
- ◆ 流控：无。

在配置 PC 机的超级终端时只需保证端口属性的配置参数与上述参数相匹配即可。以 Windows 环境下的 Hyper Terminal 为例配置 COM1 端口属性的对话框，如图 2-2 所示。

图 2-2　COM1 属性

2. 交换机的启动

在配置好终端仿真软件后，终端窗口就会显示交换机的启动信息，显示交换机的版权信息和软件加载过程，直到出现提示用户设置登录密码。

```
BIOS loading …
…
Enter Password:
Confirm Password:
<HUAWEI>
```

完成 Console 登录密码设置后，用户便可以配置和使用交换机。

3. 交换机的基本配置

在默认配置下，所有接口处于可用状态，并且都属于 VLAN1，这种情况下交换机就可以正常工作了。但为了方便管理和使用，首先应对交换机做基本的配置。

配置交换机的设备名称、管理 VLAN 和 TELNET，在对网络中交换机进行管理时需要对交换机进行基本配置。

```
<HUAWEI>
<HUAWEI> system-view
[HUAWEI] vlan 5  //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
```

```
[HUAWEI] telnet server enable   //Telnet 出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4   //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet    //V2R6 及之前版本缺省支持 telnet
//协议，但是 V2R7 及之后版本缺省的是 SSH 协议，因此使用 telnet 登录之前，必须要先配置这条命令
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
//配置管理员 Telnet 登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15 //将管理员的账号权限设置为15(最高)
```

2.1.2　典型例题分析

例 1　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】某学校计划部署园区网络，本部和分校区地理分布如图 2-3 所示。

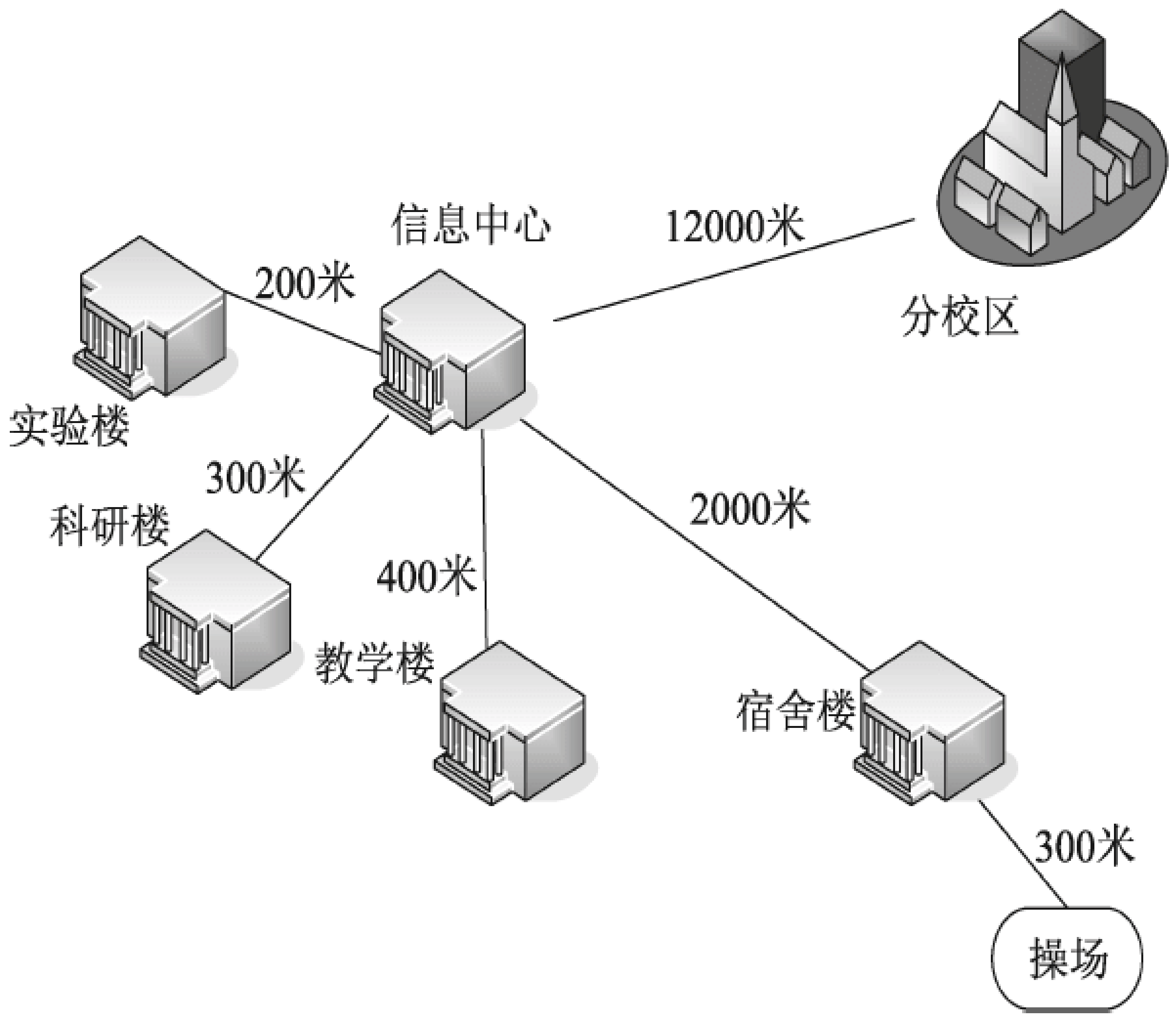


图 2-3　本校和分校区地理分布

根据需求分析结果，网络规划部分要求如下。

1. 网络中心机房在信息中心。
2. 要求汇聚交换机到核心交换机以千兆链路聚合。
3. 核心交换机要求电源、引擎双冗余。
4. 信息中心与分校区实现互通。

【问题 1】(4 分)

网络分析与设计过程一般采用五个过阶段：需求分析、通信规范分析、逻辑网络设计、物理网络设计与网络实施。其中确定新网络所需的通信量和通信模式属于__(1)__阶段；确定 IP 地址分配方案属于__(2)__阶段；明确网络物理结构和布线方案属于__(3)__阶段；确定网络投资规模属于__(4)__阶段。

【问题 2】(9 分)

根据需求分析，规划该网络拓扑如图 2-4 所示。

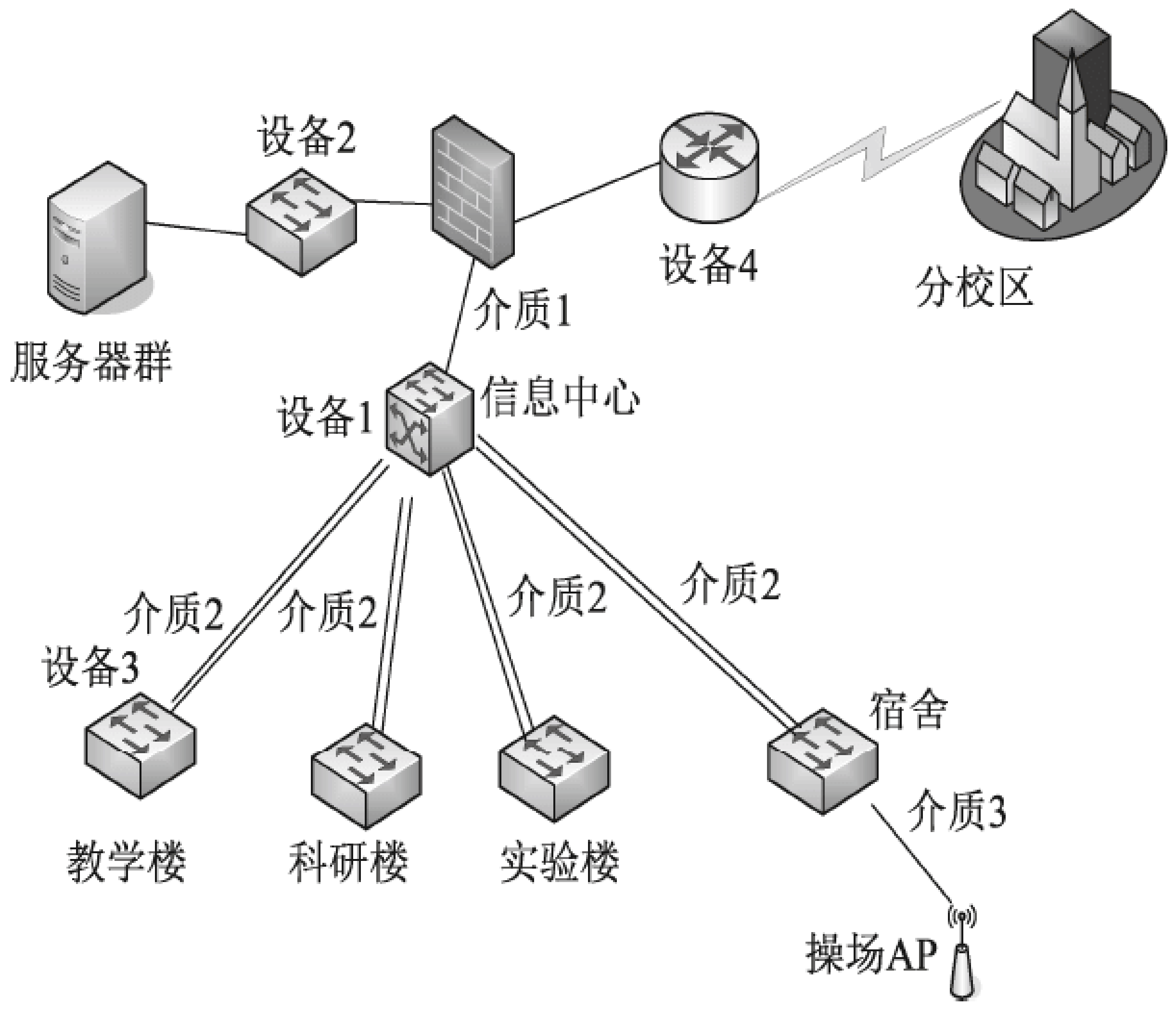


图 2-4 网络拓扑图

1. 核心交换机配置如表 2-1 所示，确定核心交换机所需配备的模块最低数量。

表 2-1 核心交换机配置

设备大类	模块描述	数 量
核心交换机	以太网交换机主机	1
	交换路由引擎	(5)
	交流电源模块，1400W	(6)
	24 端口千兆以太网电接口板(RJ-45)	1
	12 端口千兆以太网光接口板(SFP，LC)	(7)
	SFP-GE 模块(1310nm，LC)	(8)

2. 根据网络需求描述、网络拓扑结构、核心交换机设备表，图 2-4 中的介质 1 应选用 (9) ，介质 2 应选用 (10) ，介质 3 应选用 (11) 。

问题(9)～(11)备选答案：(注：每项只能选择一次)

A. 单模光纤　B. 多模光纤　C. 6 类双绞线　D. 同轴电缆

3. 为了网络的安全运行，该网络部署了 IDS 设备。在图 2-4 的设备 1、2、3、4 上，适合部署 IDS 设备的是 (12) 及 (13) 。

【问题 3】(4 分)

该校园根据需要部署了两处无线网络：一处位于学校操场；一处位于科研楼。其中操场的无线 AP 只进行用户认证，科研楼的无线 AP 只进行指定用户的接入。

1. 无线 AP 分为 FIT AP 和 FAT AP 两种。为了便于集中管理，学校的无线网络采用了无线网络控制器，所以该学校的无线 AP 为 (14) AP。天线通常分为全向天线和定向天线，为保障操场的无线覆盖范围，此时应配备 (15) 天线。

2. 为了保证科研楼的无线 AP 的安全性，根据需求描述，一方面需要进行用户认证，另一方面还需要对接入终端的 (16) 地址进行过滤，同时为保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和 WPA2 三种方式。目前，安全性最好的是 (17) 。

【问题 4】(3 分)

学校计划采用 VPN 方式实现分校区与本部的互通。VPN 的隧道协议主要有三种：PPTP、L2TP 和 IPSec，其中__(18)__和__(19)__协议工作在 OSI 模型的第二层，又称为二层隧道协议；__(20)__是第三层隧道协议。

答案：

【问题 1】

(1) 通信规范分析

(2) 逻辑网络设计

(3) 物理网络设计

(4) 需求分析

【问题 2】 (5) 2 个　(6) 2 个　(7) 1 个　(8) 8 个　(9) C　(10) A　(11) B　(12) 设备 2　(13) 设备 1

【问题 3】 (14) FIT　(15) 全向　(16) MAC　(17) WPA2

【问题 4】 (18) PPTP　(19) L2TP　(20) IPSec

解析：

【问题 1】 其中，确定新网络所需的通信量和通信模式属于通信规范分析阶段。逻辑设计过程主要由 4 个步骤组成：确定逻辑设计目标、网络服务评价、技术选项评价、进行技术决策。确定 IP 地址分配方案属于逻辑网络设计阶段。物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。因此明确网络物理结构和布线方案属于物理网络设计阶段；确定网络投资规模属于需求分析阶段。

【问题 2】 根据题干描述可知，核心交换机要求电源、引擎双冗余，而且要求汇聚交换机到核心交换机以千兆链路聚合。所以核心交换机的交换路由引擎及交流电源模块最低数量为 2 个。根据拓扑结构图，核心交换机下共有 4 个汇聚交换机，而汇聚交换机到核心交换机以千兆链路聚合，所以光模块-SFP-GE-单模模块最少需要 8 个，12 端口千兆/百兆以太网光接口模块最少需要 1 个。

根据网络需求描述、网络拓扑结构、核心交换机设备表，由于备选答案每项只能选择一次，故先判断介质 2 必须选择单模光纤，介质 3 只能选择多模光纤，所以介质 1 只能选择 6 类双绞线。

入侵检测系统是一个监听设备，无须跨接在任何链路上，不产生任何网络流量便可以工作。因此，部署 IDS 的唯一的要求是，应当挂接在所关注流量必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量，以及需要统计、监视的网络报文。目前的网络都是交换式的拓扑结构，因此一般选择在尽可能靠近攻击源，或者尽可能接近受保护资源的地方，这些位置通常是：服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上。所以，在图 2-4 中的设备 1、2、3、4 中，适合部署 IDS 设备 1 和设备 2。

【问题 3】 FAT AP 无线网路解决方案可由 FAT AP 直接在有线网的基础上构成，所有 AP 都单独进行配置，且难以集中管理；而 FIT AP 无线网络解决方案则是由无线网路控制器和 FIT AP 在有线网的基础上构成，且 FIT AP 上“零配置”，所有配置都集中到无线网络控制器上，易于集中管理。室外全向天线将信号均匀分布在中心点周围 360° 全方位区域，

要架在较高的地方，适用于连接点距离较近，分布角度范围大，且数量较多的情况。室外的定向天线的能量聚集能力最强，信号的方向指向性极好。因此，本题应该配备全向天线。为了保证科研楼的无线 AP 的安全性，根据需求描述，一方面需要进行用户认证，另一方面还需要对接入终端的 MAC 地址进行过滤，同时为保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和WPA2 三种方式。目前，安全性最好的是 WPA2。古老的“WEP”加密方式，在安全上存在着若被第三者恶意截获信号密码容易被破解的问题。WPA2 是 WPA 的升级版，现在新型的网卡，AP 都支持 WPA2 加密。WPA2 则采用了更为安全的算法。

【问题 4】 二层隧道协议主要有三种：PPTP(Point to Point Tunneling Protocol，点对点隧道协议)、L2F(Layer 2 Forwarding，二层转发协议)和 L2TP(Layer 2 Tunneling Protocol，二层隧道协议)。其中 L2TP 结合了前两个协议的优点。

三层隧道协议：用于传输三层网络协议的隧道协议，主要有 GRE 和 IPSec。

例 2 阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】 某学校有 3 个校区，校区之间最远距离达到 61 千米，学校现在需要建设校园网，具体要求如下：校园网通过多运营商接入互联网，主干网采用千兆以太网将 3 个校区的中心节点连起来，每个中心节点都有财务、人事和教务 3 类应用。按应用将全网划分为 3 个 VLAN，3 个中心都必须支持 3 个 VLAN 的数据转发。路由器用光纤连到校区 1 的中心节点上，距离不超过 500 米，网络结构如图 2-5 所示。

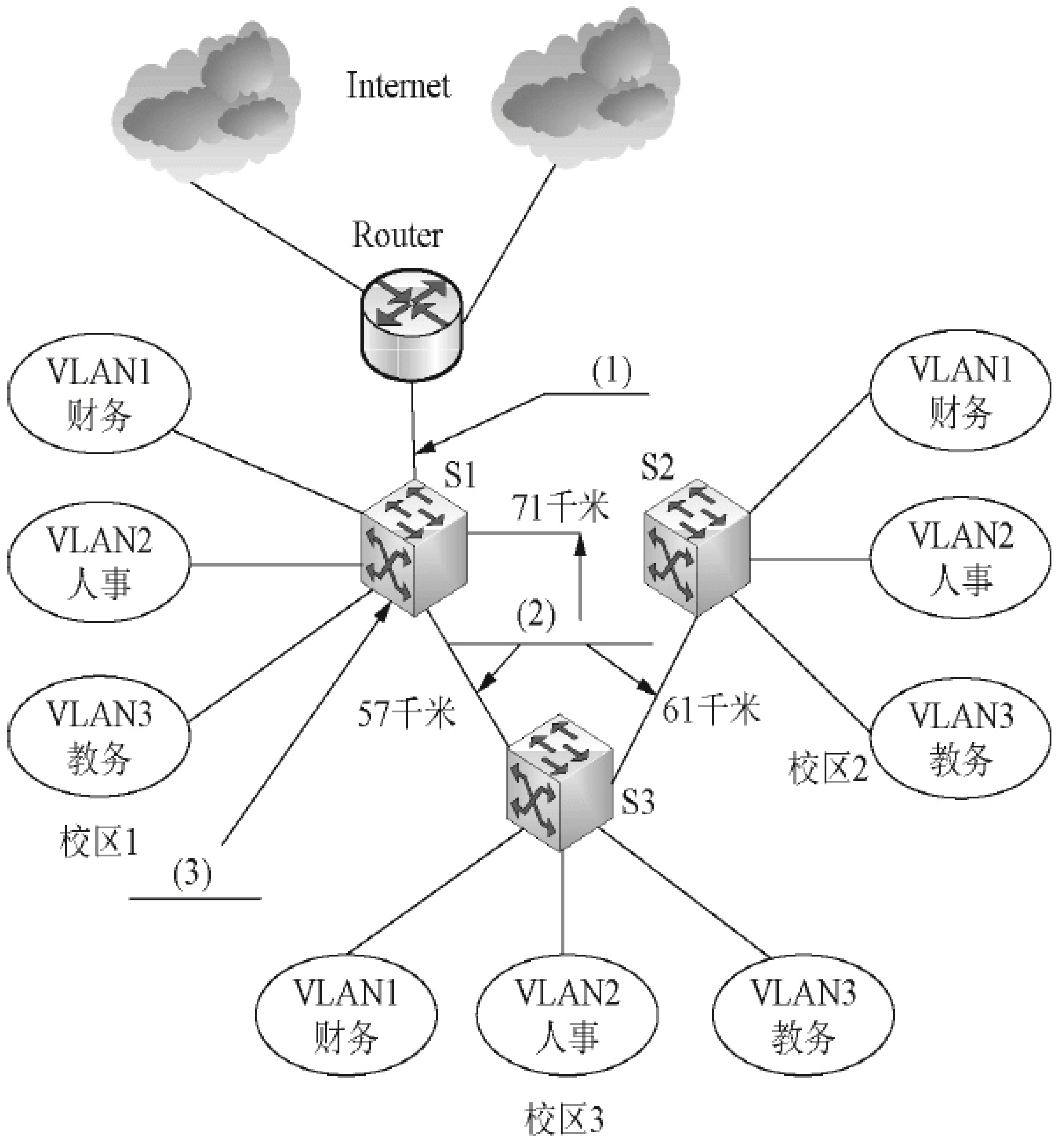


图 2-5 网络拓扑图

【问题 1】(3 分)

根据题意和图 2-5，从经济性和实用性出发填写网络拓扑图中所用的传输介质和设备。

空(1)～(3)备选答案：

A. 3 类 UTP	B. 5 类 UTP	C. 6 类 UTP
D. 单模光纤	E. 多模光纤	F. 千兆以太网交换机

G. 百兆以太网交换机　　H. 万兆以太网交换机

【问题 2】(4 分)

如果校园网中办公室用户没有移动办公的需求，采用基于 (4) 的 VLAN 划分方法比较合理；如果有的用户需要移动办公，采用基于 (5) 的 VLAN 划分方法比较合适。

【问题 3】(6 分)

图 2-5 中所示的交换机和路由器之间互连的端口类型全部为标准的 GBIC 端口，表 2-2 列出了互连所用的光模块的参数指标，请根据组网需求从表 2-4 中选择合适的光模块类型满足合理的建网成本，Router 和 S1 之间用 (6) 互连，S1 和 S2 之间用 (7) 互连，S1 和 S3 之间用 (8) 互连，S2 和 S3 之间用 (9) 互连。

表 2-2　光模块的参数指标

光模块类型	支持的参数指标			
	标　准	波长/nm	光纤类型/μm	备　注
模块 1	1000 BaseSX	850	62.5/125 50/125	多模，价格便宜
模块 2	1000 BaseLX/1000BaseLH	1310	62.5/125 50/125 9/125	单模，价格稍高
模块 3	1000 BaseZX	1550	9/125	单模，价格昂贵

【问题 4】(3 分)

如果将 Router 和 S1 之间互连的模块与 S1 和 S2 之间的模块互换，Router 和 S1 以及 S1 和 S2 之间的网络是否能连通？

【问题 5】(4 分)

若 VLAN3 的网络用户因为业务需要只允许从 ISP1 出口访问 Internet，在路由器上需进行基于 (10) 的策略路由配置。其他 VLAN 用户访问 Internet 资源时，若访问的是 ISP1 上的网络资源，则从 ISP1 出口；若访问的是其他网络资源，则从 ISP2 出口，那么在路由器上需进行基于 (11) 的策略路由配置。

答案：

【问题 1】

(1) E　(2) D　(3) F

【问题 2】

(4) 交换机端口　(5) MAC 地址

【问题 3】

(6) 模块 1　(7) 模块 2　(8) 模块 3　(9) 模块 3

【问题 4】

Router 与 S1 通，S1 与 S2 不通，因为模块 2 的传输介质兼容多模光纤，模块 1 的传输介质不兼容单模光纤。

【问题 5】

(10) 源地址　(11) 目的地址

解析：

【问题 1】(1)题中说明路由器用光纤连接到校区 1 的中心节点上，距离不超过 500 米，应采用多模光纤。(2)题中校区之间最远距离达到 61 千米，且网络要求千兆干线，所以应采用单模光纤。(3)题中要求用千兆以太网将 3 个校区的中心节点连起来，故此处应为千兆以太网交换机。

【问题 2】 根据端口来划分 VLAN：许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定的端口都在同一个广播域中。根据 MAC 地址划分 VLAN：对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置。

【问题 3】 Router 和 S1 之间是多模光纤，故直接选用模块 1；S1 和 S2 之间是单模光纤，距离 71 千米，选用价格稍高的模块 2 即可；S1 和 S3 以及 S2 和 S3 之间是单模光纤，距离分别为 57 千米、61 千米，选用价格昂贵的模块 3。

【问题 4】 Router 与 S1 通，S1 与 S2 不通，因为模块 2 的传输介质兼容多模光纤，模块 1 的传输介质不兼容单模光纤。

【问题 5】 若只允许从 ISP1 出口访问 Internet，则在路由器上进行基于源地址的策略路由配置。若访问的是其他资源，则进行基于目的地址的配置。

例 3 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】某单位网络结构如图 2-6 所示，其中维护部通过 DDN 专线远程与总部互通。

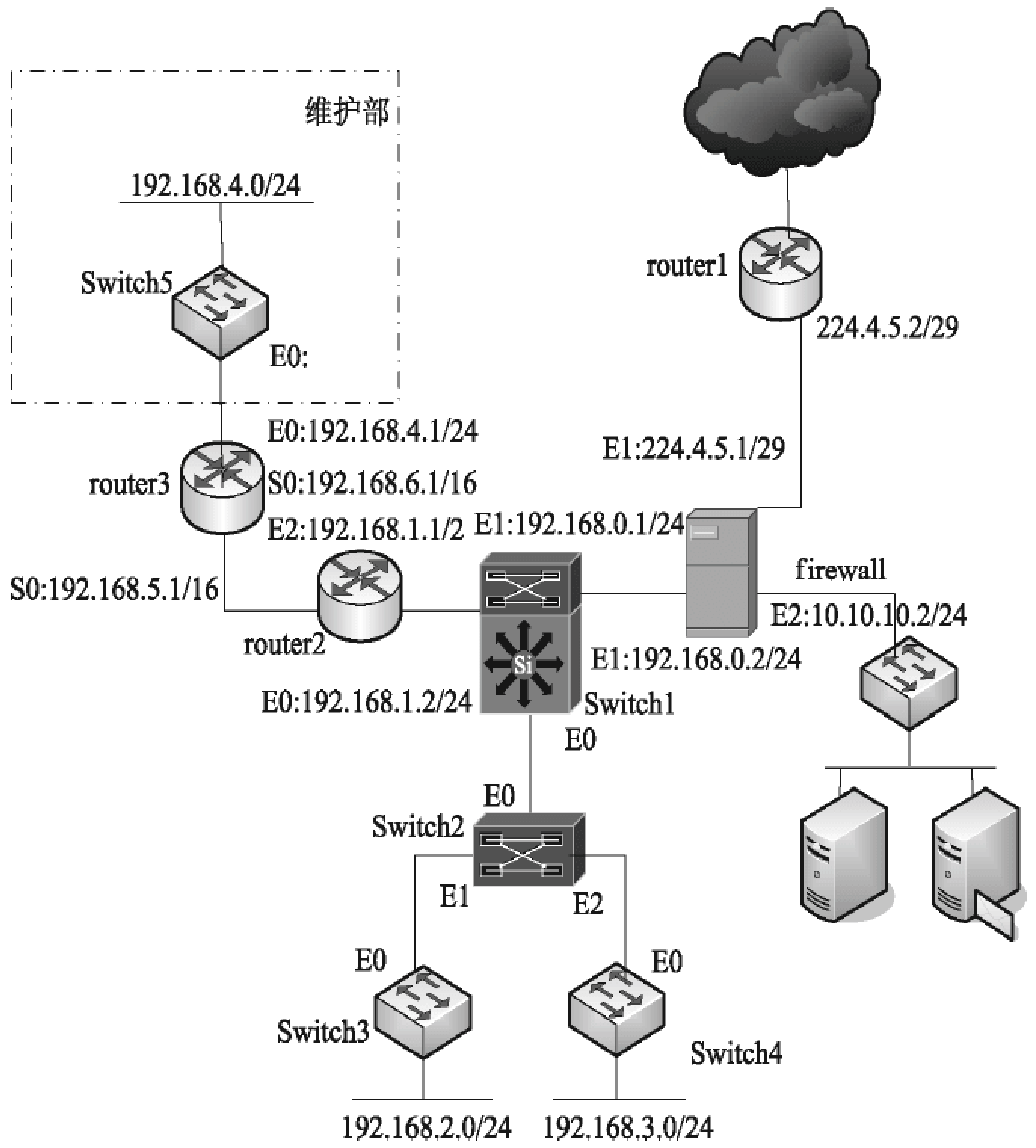


图 2-6　网络拓扑图

【问题 1】(3 分)

核心交换机 Switch1 的部分配置如下，请根据说明和网络拓扑图完成下列配置。

```
…
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 2
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 3
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 4
Switch1(config-if)#ip address 192.168.3.1 255.255.255.0
Switch1(config-if)#no shutdown
…
Switch1(config-router) #ip route 0.0.0.0 0.0.0.0 __(1)__
Switch1(config)#ip route __(2)__ 255.255.255.0 __(3)__
…
```

【问题 2】(3 分)

根据网络拓扑和需求说明，完成汇聚交换机 Switch2 的部分配置。

```
Switch2(config)#interface fastEthernet 0/0
Switch2(config-if)#switchport mode __(4)__
Switch2(config-if)#no shutdown
Switch2(config)#interface fastEthernet 0/1
Switch2(config-if)#switchport mode __(5)__
Switch2(config-if)#switchport access __(6)__
Switch2(config-if)#no shutdown
```

【问题 3】(9 分)

根据网络拓扑和需求说明，完成(或解释)路由器 router2 的部分配置。

```
…
R2(config-if)#interface ethernet0
R2(config-if)#ip address __(7)__ __(8)__
R2(config-if)#no shutdown
R2(config-if)#interface Serial0
R2(config-if)#ip address __(9)__ __(10)__
R2(config-if)#no shutdown
…
R2(config)#ip route 0.0.0.0 0.0.0.0 __(11)__
R2(config)#ip route __(12)__ 255.255.255.0 __(13)__
R2(config)#snmp-server community publicr ro// __(14)__
R2(config)#snmp-server community publicw rw// __(15)__
…
```

【问题 4】(5 分)

按照图 2-6 所示，设置防火墙各接口的 IP 地址，并根据配置说明，完成下面的命令。

```
PIX(config)#interface ethernet0 auto
PIX(config)#interface ethernet1 100full
PIX(config)#interface ethernet2 100full
PIX(config)#ip address outside __(16)__ __(17)__              //设置外网接口 IP
PIX(config)#ip address inside 192.168.0.2 255.255.255.0    //设置内网接口 IP
PIX(config)#ip address dmz __(18)__ 255.255.255.0           //设置 DMZ 接口
PIX(config)#global (outside)1 224.4.5.1-224.4.5.6//指定公网地址范围，定义地址池
PIX(config)# __(19)__ //表示内网的所有主机都可以访问外网
```

```
PIX(config)#route outside 0 0 (20) //设置默认路由
```

答案：

【问题 1】

(1) 192.168.0.2　(2) 192.168.4.0　(3) 192.168.1.2

【问题 2】

(4) trunk　(5) access　(6) vlan 3

【问题 3】

(7) 192.168.1.2　(8) 255.255.255.0　(9) 192.168.5.1　(10) 255.255.0.0

(11) 192.168.1.1　(12) 192.168.4.0　(13) 192.168.6.1

(14) 设置 snmp-server 的只读团体名为 publicr

(15) 设置 snmp-server 的读写团体名为 publicw

【问题 4】

(16) 224.4.5.1　(17) 255.255.255.248　(18) 10.10.10.2

(19) nat(inside) 1 0 或 nat(inside)1 0.0.0.0 0.0.0.0　(20) 224.4.5.2

解析：

【问题 1】 配置默认路由，使访问外网任意流量的下一跳指向 192.168.0.2；配置静态路由，使访问 192.168.4.0 网段的流量下一跳指向 192.168.1.2。

【问题 2】 交换机 Switch2 的端口工作在帧中继模式下，空(4)为配置 Trunk 模式。空(5)是配置端口模式，故填 access；空(6)处要求把端口分配给 VLAN 3，故填 vlan 3。

【问题 3】 空(7)处为 E0 端口的 IP 地址 192.168.1.2/24，子网掩码为 255.255.255.0；空(9)处为 S0 端口的 IP 地址 192.168.5.1/16，子网掩码为 255.255.0.0；空(11)处配置默认路由，使访问外网任意流量的下一跳指向 192.168.1.1；空(12)、(13)处是配置静态路由，使访问 192.168.4.0 网段的流量下一跳指向 192.168.6.1; publicr ro 即设置 snmp-server 的读写团体名为 publicr；publicw rw 即设置 snmp-server 的读写团体名为 publicw。

【问题 4】 设置外网接口 IP 为 224.4.5.1/29，子网掩码为 255.255.255.248；设置 DMZ 接口 IP 为 10.10.10.2/24，子网掩码为 255.255.255.0；设置内网主机都可访问外网的命令为 nat(inside) 1 0；设置默认路由为 224.4.5.2/29。

例 4 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某学校计划部署校园网络，其建筑物分布如图 2-7 所示。

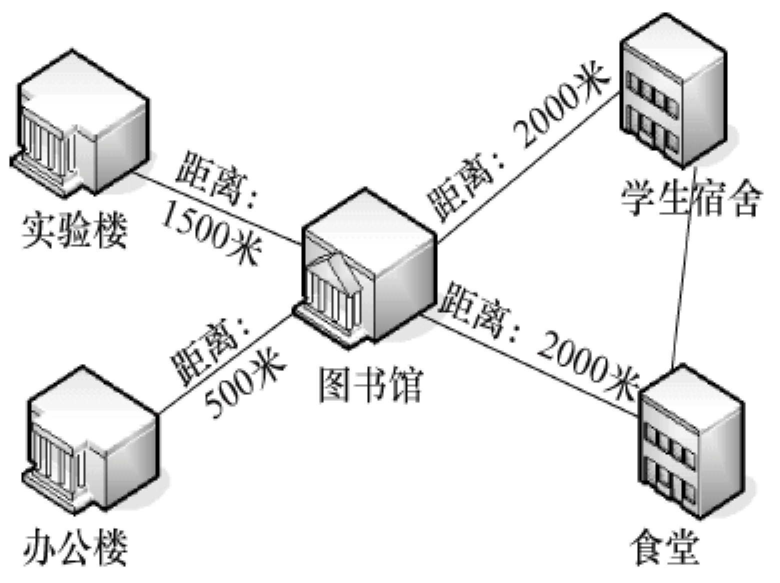


图 2-7 建筑物分布图

根据需求分析结果，校园网规划要求如下。

(1) 信息中心部署在图书馆。

(2) 实验楼部署 237 个点，办公楼部署 87 个点，学生宿舍部署 422 个点，食堂部署 17 个点。

(3) 为满足以后应用的需求，要求核心交换机到汇聚交换机以千兆链路聚合，同时千兆到桌面。

(4) 学校信息中心部署服务器，根据要求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务。

(5) 部署流控网关对 P2P 流量进行限制，以保证正常上网需求。

【问题 1】

根据网络需求，设计人员设计的网络拓扑结构如图 2-8 所示。

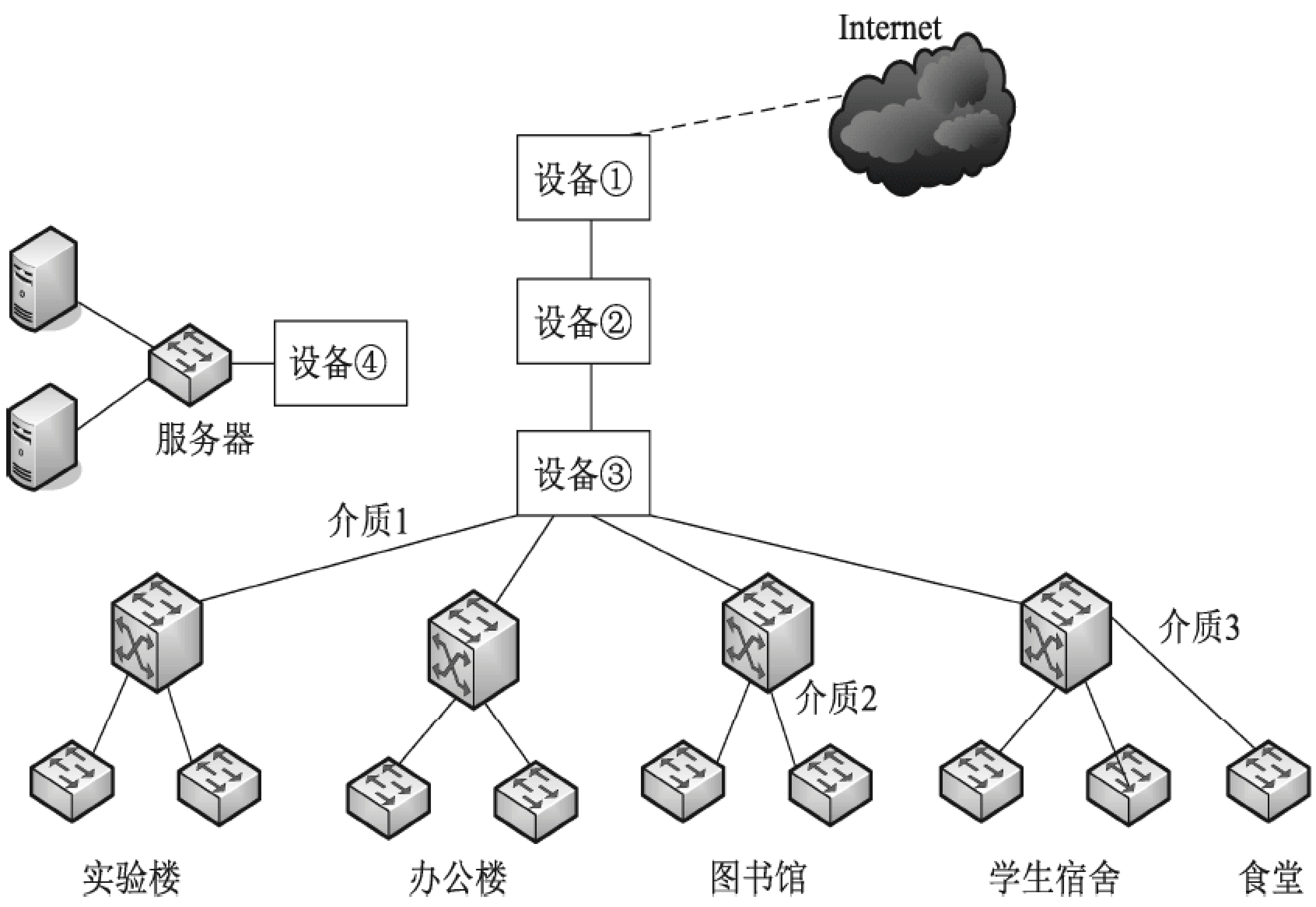


图 2-8　网络拓扑结构图

请根据网络需求描述和网络拓扑结构回答以下问题。

图 2-8 中设备①应为__(1)__，设备②应为__(2)__，设备③应为__(3)__，设备④应为__(4)__。

A. 路由器　　B. 核心交换机　　C. 流控服务器　　D. 防火墙

设备④应该接在__(5)__上。

【问题 2】

根据题目说明和网络拓扑图，在图 2-8 中，介质 1 应选用__(6)__，介质 2 应选用__(7)__，介质 3 应选用__(8)__。

A. 单模光纤　　B. 多模光纤　　C. 6 类双绞线　　D. 5 类双绞线

根据网络需求分析和网络拓扑结构图，所有接入交换机都直接连接汇聚交换机，本校园网中至少需要__(9)__台 24 口的接入交换机(不包括服务器使用的交换机)。

【问题 3】

交换机的选型是网络设计的重要工作，而交换机的背板带宽、包转发率和交换容量是其重要技术指标。其中，交换机进行数据包转发的能力称为__(10)__，交换机端口处理器和数

据总线之间单位时间内所能传输的最大数据量称为 (11) 。某交换机有 24 个固定的千兆端口，其端口总带宽为 (12) Mbps。

【问题 4】

根据需求分析，图书馆需要支持无线网络接入，其部分交换机需要提供 POE 功能，POE 的标准供电电压值为 (13) 。

A. 58 V　　B. 12 V　　C. 48 V　　D. 110 V

答案：

【问题 1】

(1) A 或路由器　(2) C 或流控服务器　(3) B 或核心交换机　(4) D 或防火墙

(5) 核心交换机或设备③

【问题 2】

(6) A 或单模光纤　(7) C 或 6 类双绞线　(8) B 或多模光纤　(9) 35

【问题 3】

(10) 包转发率　(11) 背板带宽　(12) 48 000

【问题 4】

(13) C 或 48V

解析：

【问题 1】路由器是工作在 OSI 标准模型的第三层——网络层的数据包转发设备，它通过转发数据包来实现网络互连。路由器通常连接两个或多个由 IP 子网或点到点协议标识的逻辑端口，至少拥有 1 个物理端口。而设备①起到的作用是将此 IP 子网连接到网络中去，所以设备①应为路由器。

由于网络要求部署流控网关对 P2P 流量进行限制，以保证正常上网需求，所以设备②是流控服务器。

设备③是核心交换机，连接局域网接入交换机。

信息中心部署在图书馆，学校信息中心部署服务器，根据要求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务，所以应对信息中心部署防火墙，即设备④为防火墙，部署在核心交换机上。

【问题 2】常用传输介质的特性如表 2-3 所示。

表 2-3　传输介质的特性表

传输介质	子　类	特点及应用
双绞线	3 类 UTP	10 Base-T(10 M)、令牌环(16 M)、电话
	5 类 UTP	100 Base-T (100 M)
	超 5 类 UTP	100 Base-T(100 M)、ATM(155 M)
	6 类 UTP	1000 Base-T(1000 M)
	STP	外加屏蔽层，施工困难

续表

传输介质	子　类	特点及应用
同轴电缆	基带同轴电缆	阻抗 50 Ω，细缆用于 10 Base-2，粗缆用于 10 Base-5
	宽带同轴电缆	阻抗 75 Ω，用于 CATV
光纤	多模光纤	适合于近距离传输，价格便宜
	单模光纤	较高的传输率、较长的传输距离、较高的成本

因为要求核心交换机到汇聚交换机以千兆链路聚合，同时千兆到桌面，所以将 5 类 UTP 排除。介质 1 连接核心交换机和接入交换机，传输距离较长，需要较高的传输率，所以使用单模光纤；介质 2 连接网络接入交换机和内部接入交换机，为短距离传输，所以使用 6 类 UTP；食堂到宿舍的接入交换机为近距离传输，可使用多模光纤。

由于实验楼、办公楼、图书馆、学生宿舍分别有一个接入交换机，总共需要 4 个网络接入交换机。实验楼 237 个点，需要 10 个内部接入交换机；办公楼 87 个点，需要 3 个内部接入交换机；学生宿舍 422 个点，需要 18 个内部接入交换机；食堂直接用其他剩余端口，则总共需要的交换机数目为 4+10+3+18=35。

【问题 3】 包转发率是指基于 64 字节分组，在单位时间内交换机转发的数据总数。转发速率体现了交换引擎的转发性能。端口吞吐量反映端口的分组转发能力。交换机背板是设计值，可以大于等于交换容量(此为达到线速交换机的一个标准)。厂家在设计的时候考虑了将来模块的升级，比如模块从开始的百兆升级到支持千兆、万兆，端口密度增加等。背板带宽多指模块化交换机。它决定了各模板与交换引擎间的连接带宽的最高上限，是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。背板带宽标志了交换机总的数据交换能力，单位为 Gbps，也叫交换带宽。

总带宽=端口数×端口速率×2(全双工模式)，所以总带宽为 24×1000 Mbps×2=48 000 Mbps。

【问题 4】 空(13)POE 标准供电系统的主要供电特性参数为：

① 电压在 44～57 V，典型值为 48 V。

② 允许最大电流为 550 mA，最大启动电流为 500 mA。

③ 典型工作电流为 10～350 mA，超载检测电流为 350～500 mA。

④ 在空载条件下，最大需要电流为 5 mA。

⑤ 为 PD 设备提供 3.84～12.95 W 五个等级的电功率请求，最大不超过 13 W。

2.1.3　同步练习

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】某学校计划建立校园网，拓扑结构如图 2-9 所示。该校园网分为核心、汇聚、接入三层，由交换模块、广域网接入模块、远程访问模块和服务器群四大部分构成。

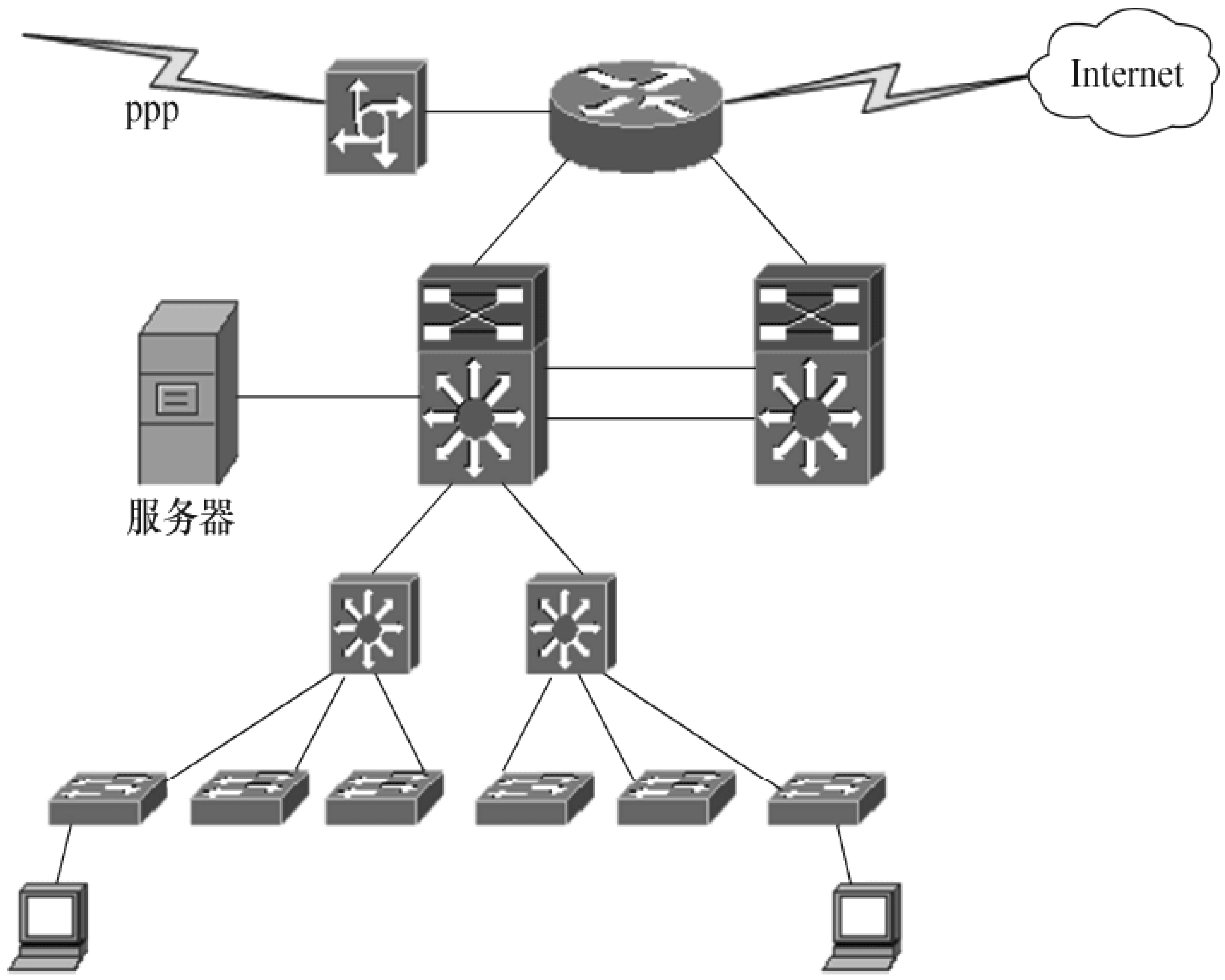


图 2-9　网络拓扑结构图

【问题 1】(5 分)

在校园网设计过程中，划分了很多 VLAN，采用了 VTP 来简化管理。将(1)～(5)处空缺信息填写在答题纸对应的解答栏内。

VTP 信息只能在__(1)__端口上传播。

运行 VTP 的交换机可以工作在三种模式下：__(2)__、__(3)__、__(4)__。

共享相同 VLAN 数据库的交换机构成一个__(5)__。

【问题 2】(4 分)

该校园网采用了异步拨号进行远程访问，异步封装协议采用了 PPP 协议。将(6)～(9)处空缺信息填写在答题纸对应的解答栏内。

异步拨号连接属于远程访问中的电路交换服务，远程访问中另外两种可选的服务类型是：__(6)__和__(7)__。

PPP 提供了两种可选的身份认证方法，它们分别是__(8)__和__(9)__。

【问题 3】(2 分)

该校园网内交换机的数量较多，交换机间链路复杂，为了防止出现环路，需要在各交换机上运行__(10)__。

【问题 4】(4 分)

该校园网在安全设计上采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、内部网络访问控制层、操作系统及应用软件层和数据存储层，对各层的安全采取不同的技术措施。从备选答案中选择信息，将(11)～(14)处空缺信息填写在答题纸对应的解答栏内。

安全技术	对应层次
__(11)__	外部网络传输控制层
__(12)__	内外网间访问控制层
__(13)__	内部网络访问控制层
__(14)__	数据存储层

(11)～(14)备选答案：

A. IP 地址绑定　　B. 数据库安全扫描

C. 虚拟专用网(VPN)技术　　D. 防火墙

2.1.4　同步练习参考答案

答案：

【问题 1】

(1)　Trunk

(2)　VTP Server 或服务器模式

(3)　VTP Client 或客户端模式

(4)　VTP Transparent 或透明模式

说明：(2)、(3)、(4)处答案次序任意。

(5)　VTP 管理域

【问题 2】

(6)　专线连接

(7)　分组交换

说明：(6)、(7)处答案可以互换。

(8)　口令认证协议(Password Authentication Protocol，PAP)

(9)　质询握手认证协议(Challenge Handshake Authentication Protocol，CHAP)

说明：(8)、(9)处答案可以互换。

【问题 3】

(10) 生成树协议(Spanning Tree Protocol，STP)

【问题 4】

(11) C 或虚拟专用网(VPN)技术

(12) D 或防火墙

(13) A 或 IP 地址绑定

(14) B 或数据库安全扫描

2.2　VLAN 的配置

2.2.1　考点辅导

虚拟局域网(Virtual Local Area Network，VLAN)技术的出现和局域网交换技术是分不开的。局域网交换技术使用户抛弃了传统的总线技术，并在一定范围内代替了人们早已熟知的共享型介质。

VLAN 为本地网提供了一种解决方案。VLAN 中仍然需要路由器，仍然存在着广播流量。不同的是，在我们将交换技术和 VLAN 技术相结合后，网段中的用户可以很少，甚至可以只有一个用户(一台主机)，而广播域则能大到包含上千个用户。另外，如果使用得当，VLAN 中的工作站可以移动到新的物理位置而不需要重新配置任何参数。

2.2.1.1　VLAN 的功能

VLAN 是指在交换局域网的基础上，采用网络管理软件构建可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备。要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

在使用带宽、灵活性、性能等方面，VLAN 都显示出很大优势。在 VLAN 中能够方便地进行用户的增加、删除、移动等操作，提高网络管理的效率。VLAN 具有以下功能。

1. 控制广播风暴

一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。广播流量被限制在软定义的边界内，从而提高了网络的安全性。

2. 提高网络整体安全性

通过路由访问列表和 MAC(传输媒体访问控制)地址分配 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同的 VLAN 中，从而提高交换式网络的整体性能和安全性。此外，在相同 VLAN 内的主机间传送的数据不会影响到其他 VLAN 上的主机，因此减少了数据窃听的可能性，极大地增强了网络的安全性。

3. 网络管理简单、直观

对于交换式以太网，如果对某些用户重新进行网段分配，需要网络管理员对网络系统的物理结构重新进行调整，甚至需要追加网络设备，从而增大网络管理的工作量。而对于采用 VLAN 技术的网络来说，一个 VLAN 可以根据部门职能、对象组成或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改动网络物理连接的情况下可以任意地将工作站在工作组或子网之间移动。使用 VLAN 技术，可大大减轻网络管理和维护工作的负担，降低网络维护费用。在一个交换网络中，VLAN 提供了网段和机构的弹性组合机制。

2.2.1.2　VLAN 的机制

VLAN 是一种软技术，其如何分类，将决定此技术在网络中能否发挥出预期作用。常见的 VLAN 分类有 3 种：基于端口、基于 MAC 地址和基于网络层。

1. 基于端口

基于端口的 VLAN 划分是比较流行的，也是最早的划分方式，其特点是将交换机按照端口进行分组，每一组定义为一个 VLAN。这些交换机端口分组可以在一台交换机上，也可以跨越几个交换机。

目前端口分组是定义 VLAN 成员最常用的方法，而且配置也相当直截了当。纯粹用端口分组来定义 VLAN，不容许多个 VLAN 包含同一个实际交换机端口。用端口定义 VLAN 的主要局限是：使用不够灵活，当用户从一个端口移到另一个端口时，网络管理员必须重新配置 VLAN 成员。

2. 基于 MAC 地址

基于硬件 MAC 地址定义的 VLAN 既有优点又有缺点。由于数据链路层的 MAC 地址是硬连接到工作站的网络界面卡(NIC)上的，所以基于 MAC 地址的 VLAN 使网络管理者能够把网络上的工作站移动到不同的实际位置，而且可以让这台工作站自动地保持它原有的 VLAN 成员资格。按照这种方式，由硬件 MAC 地址定义的 VLAN 可以被视为基于用户的 VLAN。

在这种方式的 VLAN 中，交换机对终端的 MAC 地址和交换机端口进行跟踪。在新终端入网时，根据已经定义的 VLAN-MAC 对应表将其划归某一个 VLAN。无论该终端在网络中怎样移动，由于其 MAC 地址保持不变，故不需进行 VLAN 的重新配置。这种划分方式减少了网络管理员的日常维护工作量，不足之处在于所有的终端必须被明确地分配在一个具体的 VLAN，任何时候增加终端或者更换网卡，都要对 VLAN 数据库进行调整，以实现对该终端的动态跟踪。

基于 MAC 地址的 VLAN 解决方案的缺点之一是要求所有的用户必须初始配置在至少一个 VLAN 中。在初始手工配置之后，用户的自动跟踪才有可能实现。然而，这种不得不在一开始就先用人工配置 VLAN 的方法的缺点在一个非常大的网络中变得非常明显：几千个用户必须逐个地分配到各自特定的 VLAN 中。

3. 基于网络层

基于网络层的 VLAN 划分也叫作基于策略(Policy)的划分，是这几种划分方式中最高级也是最复杂的。基于网络层的 VLAN 使用协议(如果网络中存在多协议的话)或网络层地址(如 TCP/IP 中的子网段地址)来确定网络成员。

在 VLAN 中应用最广的就是 VTP 和 STP 技术。VTP(VLAN Trunking Protocol)用于保持 VLAN 配置的统一性。VTP 在系统级管理 VLAN 的增加、删除、调整时，自动地将信息向网络中其他的交换机广播。此外，VTP 减少了可能导致安全问题的配置。

VTP 的运行有 3 种模式：服务器模式、客户模式和透明模式。当交换机处在 VTP 服务器模式或透明模式时，网管员能够在交换机上配置 VLAN。网管员通过使用 CLI、控制台菜单、MIB(使用 SNMP 简单网络管理协议管理工作站)来修改 VLAN 配置。

一个配置为VTP服务器模式的交换机向邻近的交换机广播VLAN配置时，它通过Trunk端口，从邻近的交换机学习新的 VLAN 配置。例如：当网络增加了一个 VLAN 时，VTP 就将广播这个新的 VLAN，服务器和客户端的 Trunk 网络端口就准备接收 VLAN 的相关信息。

在交换机自动转到 VTP 的客户模式后，它会传送广播信息，并从广播中学习新的信息。但是，它不能通过 MIB(管理信息库)控制台菜单来增加、删除、修改 VLAN。VTP 客户端不能将 VLAN 信息保存在非易失存储器(NVRAM)中。当设备启动时，它会通过 Trunk 网络端口接收广播信息，学习配置信息。

在 VTP 透明模式中，交换机不作广播或从网络学习 VLAN 配置，但可以通过控制台、CLI、MIB 来修改、增加和删除 VLAN。

为了使 VLAN 能够使用，必须使 VTP 知道其存在，并且 VLAN 的相关信息要包含在 Trunk 端口的准许列表中。一个快速以太网 Trunk 端口自动为 VLAN 传输数据，并且是从一个交换机传到另一个交换机。

而 STP(Spanning Tree Protocol)则能够提供路径冗余，并且可以使两台交换机中只有一

条有效路径。

STP 在桥接(或交换)网络中定义了一棵树，并且迫使一定的备份路径处于备用状态。如果生成树中的网络一部分不可达，或者 STP 值变化了，生成树算法会重新计算生成树拓扑，并且通过启动备份路径来重新建立连接。STP 操作对于交换机来说是透明的，而不管交换机是连在 VLAN 的某一部分还是多个部分。

当创建网络时，如果网络中所有节点都存在多条路径，则生成树中的算法可以计算出最佳路径。因为每个 VLAN 是一个逻辑局域网部分，所以网管员可以使用 STP 工作在多个 VLAN 中。

2.2.1.3 交换机的常见配置

VLAN 技术上是交换技术的重要组成部分，也是交换机配置的基础。它用于把物理上直接相连的网络从逻辑上划分为多个子网。每一个 VLAN 对应着一个广播域，处于不同 VLAN 上的主机不能进行通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置和管理主要涉及链路和接口类型、GARP 协议和 VLAN 的配置。

链路和接口类型，为了适应不同网络环境的组网需要，链路类型分为接入链路(Access Link)和干道链路(Trunk Link)两种链路类型。接入链路只能承载 1 个 VLAN 的数据帧，用于连接交换机和用户终端；干道链路能承载多个不同 VLAN 的数据帧，用于交换机间互连或连接交换机与路由器。根据接口连接对象以及对收发数据帧处理的不同，以太网接口分为 Access 接口、Trunk 接口、Hybrid 接口和 QinQ 接口四种接口类型，分别用于连接终端用户、交换机与路由器以及公网与私网的互联等。

GARP 协议主要用于建立一种属性传递扩散机制，以保证协议实体能够注册和注销该属性。简单说就是为了简化网络中配置 VLAN 的操作，通过 GVRP 的 VLAN 自动注册功能将设备上的 VLAN 信息快速复制到整个交换网，达到减少手工配置及保证 VLAN 配置正确的目的。

交换机的初始状态是工作在透明模式，有一个默认的 VLAN1，所有端口都属于 VLAN1。

1. 划分 VLAN 的方法

虚拟局域网是交换机的重要功能，通常虚拟局域网的实现形式有多种，分别是基于接口、MAC 地址、子网、网络层协议、匹配策略方式来划分 VLAN。

通过接口来划分 VLAN。交换机的每个接口配置不同的 PVID，当数据帧进入交换机时没有带 VLAN 标签，该数据帧就会被打上接口指定 PVID 的 Tag 并在指定 PVID 中传输。

通过源 MAC 地址来划分 VLAN。建立 MAC 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧时，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过子网划分 VLAN。建立 IP 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过网络层协议划分 VLAN。建立以太网帧中的协议域和 VLAN ID 的映射关系表，当收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过策略匹配划分 VLAN，实现多种组合的划分，包括接口、MAC 地址、IP 地址等。

建立配置策略，当收到的是 Untagged 帧，且匹配配置的策略时，给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

2. 配置 VLAN 举例

在网络中，用于终端与交换机、交换机与交换机、交换机与路由器连接时 VLAN 的划分方式多种多样，需要灵活运用。这里就接入层交换机的 VLAN 划分举例说明。

(1) 以接入交换机 ACC1 为例，创建 ACC1 的业务 VLAN10 和 20。

```
<HUAWEI> system-view
[HUAWEI] sysnameACC1//修改设备名称为 ACC1
[ACC1] vlan batch 10 20//批量创建 VLAN
```

(2) 配置 ACC1 连接 CORE1 和 CORE2 的 GE0/0/3 和 GE0/0/4，透传部门 A 和部门 B 的 VLAN。

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
//配置 GE0/0/3 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/4] port trunk allow-pass vlan 10 20
//配置 GE0/0/4 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/4] quit
```

(3) 配置 ACC1 连接用户的接口，使各部门加入 VLAN。

```
[ACC1] interfaceGigabitEthernet0/0/1 //配置连接部门 A 的接口
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interfaceGigabitEthernet0/0/2 //配置连接部门 B 的接口
[ACC1-GigabitEthernet0/0/2] port link-type access
[ACC1-GigabitEthernet0/0/2] port default vlan 20
[ACC1-GigabitEthernet0/0/2] quit
```

(4) 配置 BPDU 保护功能，加强网络的稳定性。

```
[ACC1] stpbpdu-protection
```

如果把 ACC1 下接入的用户都加入 VLAN 10，为了配置简单，也可以 ACC1 上不配置 VLAN，而把 CORE1、CORE2 与 ACC1 直接相连的接口以 access 方式加入 VLAN10，这样通过 ACC1 接入的用户全部属于 VLAN 10。

2.2.2　典型例题分析

【说明】(2015 年下半年下午试题一)

某公司网络拓扑结构图如图 2-10 所示。公司内部的用户使用私有地址段 192.168.1.0/24。

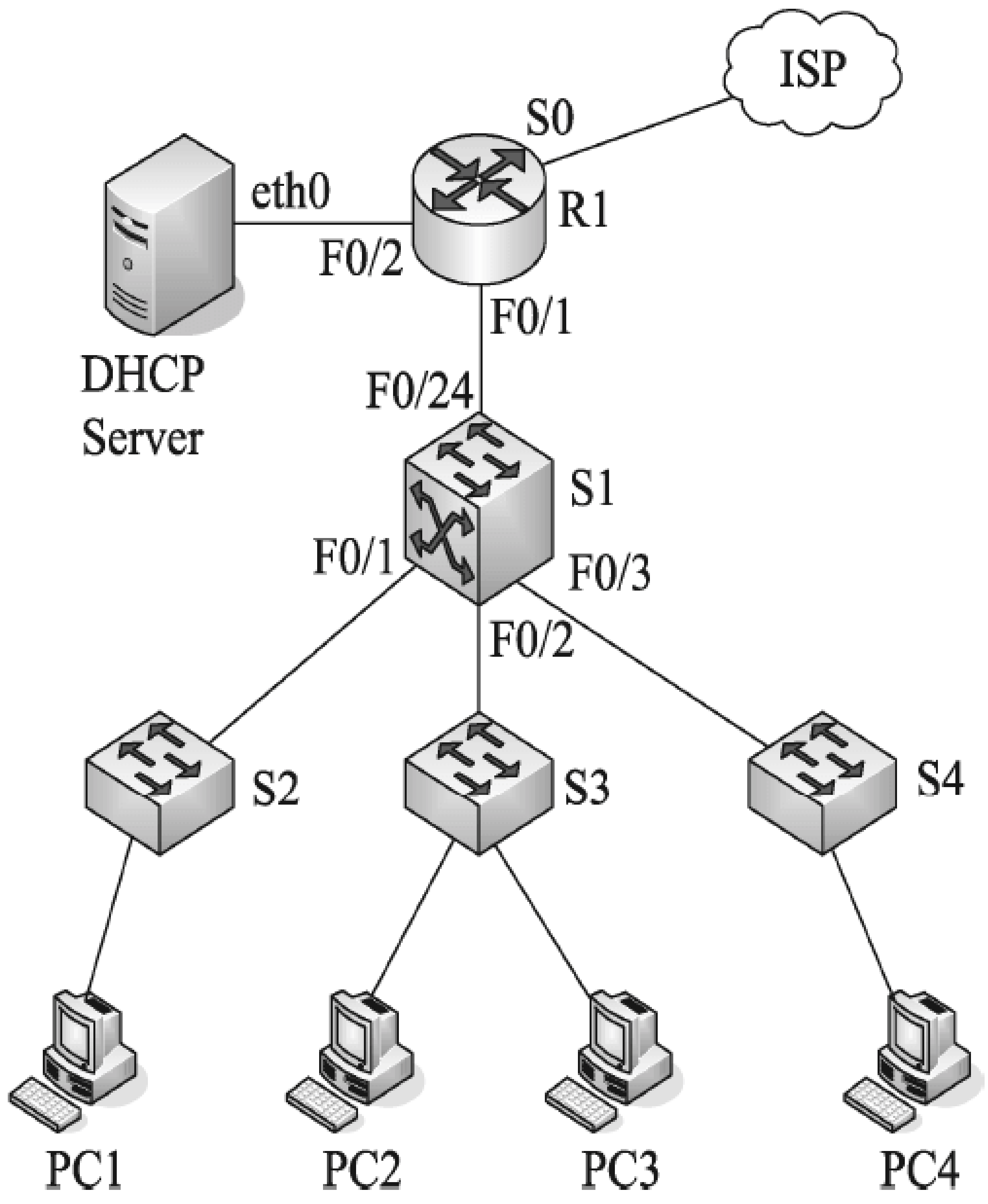


图 2-10　网络拓扑结构图

【问题 1】(2 分)

为了节省 IP 地址，在接口地址上均使用 30 位地址掩码，请补充下表中的空白。

设　备	接　口	IP 地址	设　备	接　口	IP 地址
S1	F0/24	192.168.1.253	R1	F0/1	(1)
DHCPServer	Eth0	192.168.1.249		F0/2	(2)

【问题 2】(9 分)

将公司内部用户按照部门分别划分在 3 个 vlan 中：vlan 10、vlan 20 和 vlan 30。均连接在交换机 S1 上，并通过 S1 实现 vlan 间通信，所有内网主机均采用 DHCP 获取 IP 地址。按照要求补充完成(或解释)以下配置命令。

```
Switch>en
Switch#  (3)
Switch(config)#hostname  (4)
S1(config)#interface fastEthernet 0/1
S1(config-if)# (5)  mode trunk
S1(config)#interface vlan 10       // (6)
S1(config-if)#ip address 192.168.1.206  255.255.255.240
S1(config-if)#no shutdown
S1(config-if)#ip helper-address  (7)
S1(config-if)# (8)
S1(config)#
…
S1(config)#router  (9)
S1(config-router)#version  (10)
S1(config-router)#network 192.168.1.192
S1(config-router)# network 192.168.1.208
S1(config-router)# network 192.168.1.224
```

```
S1(config-router)#__(11)__
S1#
```

【问题 3】(2 分)

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示：

Command rejected: An interface whose trunk encapsulation is "Auto" cannot be configured to "trunk" mode.

应采取__(12)__方法解决该问题。

(12) A. 在该接口上使用 no shutdown 命令后再使用该命令

B. 在该接口上启用二层功能后再使用该命令

C. 重新启动交换机后再使用该命令

D. 将该接口配置为 access 模式后再使用该命令

【问题 4】(2 分)

在 S1 上配置的三个 SVI 接口地址分别处在 192.168.1.192、192.168.1.208 和 192.168.1.224 网段，它们的子网掩码是__(13)__。

答案：

【问题 1】

(1) 192.168.1.254　　(2) 192.168.1.250

【问题 2】

(3) config terminal　　(4) S1　　(5) switchport　　(6) 进入 vlan10 中　　(7) 192.168.1.249

(8) exit　　(9) rip　　(10) 2　　(11) end

【问题 3】

(12) D

【问题 4】

(13) 255.255.255.240

解析：

【问题 1】(2 分)

为了节省 IP 地址，在接口地址上均使用 30 位地址掩码，R1 的 F0/1 和 S1 的 F0/24 在同一网络中，现在 S1 的 F0/24 地址是 192.168.1.253，子网掩码是 255.255.255.252，那么这个地址所在的可用主机地址范围是 192.168.1.253～192.168.1.254。R1 的 F0/1 就是 192.168.1.254。

同理，R1 的 F0/2 和 DHCP 的 eth0 处于同一网络，所以 R1 的 F0/2 的地址是 192.168.1.250。

【问题 2】(9 分)

(3)　Switch#config terminal //进入全局配置模式

(4)　Switch(config)#hostname S1 //将交换机命名为 S1

(5)　S1(config-if)switchport mode trunk //将端口封装为 trunk 模式

(6)　S1(config-if)#interface vlan 10//进入 Vlan 10

(7)　S1(config-if)#ip helper-address 192.168.1.249

//指定 DHCP 服务器的地址，表示通过 Ethernet0 向该服务器发送 DHCP 请求包

(8)　S1(config-if)#exit//退出接口子模式

(9) S1(config)#route rip//开启 RIP

(10) S1(config-router)#version 2//指定版本为 2，支持可变长子网掩码

(11) S1(config-router)#end//退出到特权模式

【问题 3】(2 分)

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示:

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

应采取将该接口配置为 access 模式后再使用该命令的方法解决该问题。

【问题 4】(2 分)

采用三层交换机的路由模块为 VLAN 之间做路由也是非常普遍的。由于三层交换机的路由模块和交换模块直接通过交换机的背板总线连接，所以不需要使用干道技术。只需要在三层交换机的路由模块上定义与 VLAN 数量相当的逻辑接口，并让这些接口和 VLAN 对应，为这些接口分配 IP 地址就可以了。SVI 交换机虚拟接口实现不同 VLAN 间通信的问题，每个 SVI 要和各个 VLAN 属于同一网络中。所以子网掩码是 255.255.255.240。

2.2.3 同步练习

【说明】(2015 年上半年下午试题四)

某企业的网络拓扑结构如图 2-11 所示。

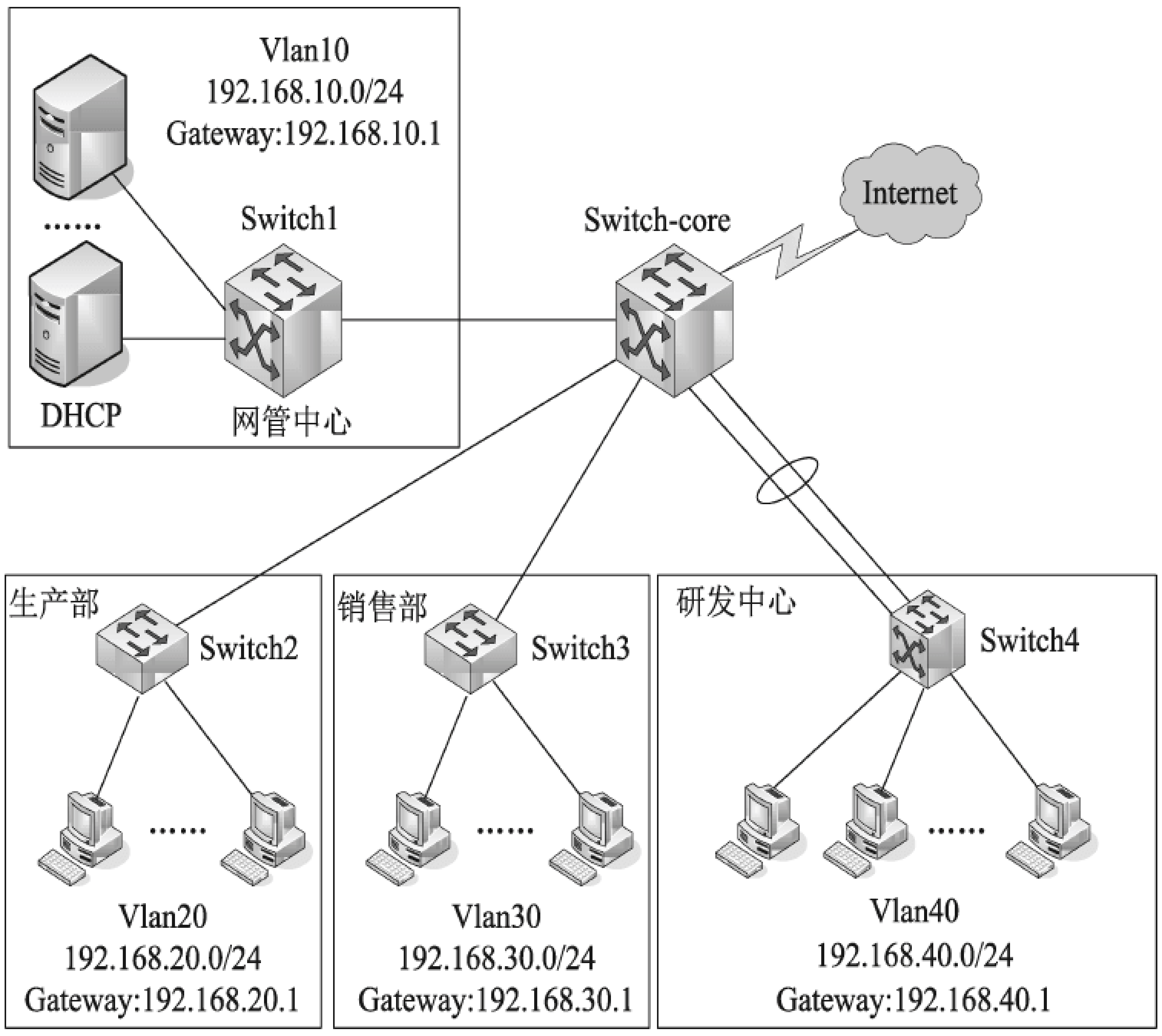


图 2-11 某企业网络拓扑结构

由于该企业路由设备数量较少，为提高路由效率，要求为该企业构建基于静态路由的多层安全交换网络。根据要求创建 4 个 VLAN 分别属于网管中心、生产部、销售部以及研发中心，各部门的 VLAN 号及 IP 地址规划如图 2-11 所示。该企业网采用三层交换机

Switch-core 为核心交换机，Switch-core 与网管中心交换机 Switch1 和研发中心交换机 Switch4 采用三层连接，Switch-core 与生产部交换机 Switch2 及销售部交换机 Switch3 采用二层互联。

各交换机之间的连接以及接口 IP 地址如表 2-4 所示。

表 2-4　各交换机之间的连接以及接口 IP 地址表

上联端口				下联端口			
交 换 机	端口	描　述	IP 地址	交换机	端口	描　述	IP 地址
Switch-core	G0/1	scsw-g1/1		Switch2	G1/1	core-g0/1	
	G0/2	scsw-g0/1	192.168.101.1/24	Switch1	G0/1	core-g0/2	192.168.101.2/24
	F0/1	yfsw-f0/1	192.168.102.1/24	Switch4	F0/1	core-f0/1	192.168.102.2/24
	F0/2	yfsw-f0/2			F0/2	core-f0/2	
	F0/3	yfsw-f0/3			F0/3	core-f0/3	
	F0/4	yfsw-f0/4			F0/4	core-f0/4	
	F0/5	xssw-f0/1		Switch3	F0/1	core-f0/5	

【问题 1】(4 分)

随着企业网络的不断发展，研发中心的上网计算机数急剧增加，在高峰时段研发中心和核心交换机之间的网络流量非常大，在不对网络进行大的升级改造的前提下，网管人员采用了以太信道(或端口聚合)技术来增加带宽，同时也起到了__(1)__和__(2)__的作用，保证了研发中心网络的稳定性和安全性。

在两台交换机之间是否形成以太信道，可以用协议自动协商。目前有两种协商协议：一种是__(3)__，是 Cisco 私有的协议；另一种是__(4)__，是基于 IEEE 802.3ad 标准的协议。

(3)、(4)备选答案：

A. 端口聚合协议(PAgP)

B. 多生成树协议(MSTP)

C. 链路聚合控制协议(LACP)

【问题 2】(7 分)

核心交换机 Switch-core 与网管中心交换机 Switch1 通过静态路由进行连接。根据需求，完成或解释 Switch-core 与 Switch1 的部分配置命令。

(1)　配置核心交换机 Switch-core。

```
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
Switch-core(config-if)#description wgsw-g0/1     //__(5)__
Switch-core(config-if)#no switchport             //__(6)__
Switch-core(config-if)#ip address __(7)__
Switch-core(config-if)#no shutdown
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
Switch-core(config)#exit
…
```

(2)　配置网管中心交换机 Switch1。

```
Switch1#config terminal
```

```
Switch1(config)#no ip domain lookup             //___(8)___
Switch1(config)#interface gigabitEthernet 0/1
Switch1(config-if)#description core-g0/2
Switch1(config-if)#no switchport
Switch1(config-if)#ip address ___(9)___
Switch1(config-if)#exit
Switch1(config)#vlan 10
Switch1(config-vlan)#name wgl0
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10               //创建 VLAN10
Switch1(config-if)#ip address ___(10)___
Switch1(config-if)#exit
Switch1(config)#interface range f0/2-20
Switch1(config-if-range)#switchport mode access    //设置端口为 access 模式
Switch1(config-if-range)#switchport access ___(11)___//设置端口所属的 VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
…
```

【问题 3】(7 分)

为确保研发中心网络的稳定性，在现有条件下尽量保证带宽，要求实现核心交换机 Switch-core 与研发中心交换机 Switch4 的三层端口聚合，然后通过静态路由进行连接。根据需求，完成或解释以下配置命令。

(1) 继续配置核心交换机 Switch-core。

```
Switch-core#config terminal
Switch-core(config)#interface port-channel 10       //___(12)___
Switch-core(config-if)#no switchport
Switch-core(config-if)#ip address___(13)___
Switch-core(config-if)#no shutdown
Switch-core(config-if)#exit
Switch-core(config)#interface range fastEthernet0/1-4  //选择配置的物理接口
Switch-core(config-if-range)#no switchport
Switch-core(config-if-range)#no ip address     //确保该物理接口没有指定的 IP 地址
Switch-core(config-if-range)#switchport       //改变该端口为 2 层接口
Switch-core(config-if-range)#channel-group 10 mode on     //___(14)___
Switch-core(config-if-range)#no shutdown
Switch-core(config-if-range)#exit
Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2
…
```

(2) 配置研发中心交换机 Switch4。

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
Switch4(config-if)#no switchport
Switch4(config-if)#ip address___(15)___
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4     //选择配置的物理接口
Switch4(config-if-range)#no switchport
Switch4(config-if-range)#no ip address
…
```

```
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)#__(16)__                    //配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yfl0
Switch4(config-vlan)#exit
Switch4(config)#__(17)__                    //开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
Switch4(config-if-range)#switchport mode access
…
Switch4(config-if-range)#_(18)_             //退回到特权模式
Switch4#
…
```

【问题 4】(2 分)

为了保障局域网用户的网络安全，防范欺骗攻击，以生产部交换机 Switch2 为例，配置 DHCP 侦听。根据需求完成或解释 Switch2 的部分配置命令。

```
Switch2#config terminal
Switch2(config)#ip dhcp snooping          //__(19)__
Switch2(config)#ip dhcp snooping vlan 20
Switch2(config)#interface gigabitEthernetl/l
Switch2(config-if)#ip dhcp snooping trust   //__(20)__
Switch2(config-if)#exit
…
```

2.2.4　同步练习参考答案

答案：

【问题 1】

(1) 负载均衡　(2) 冗余备份　(3) A　(4) C

【问题 2】

(5) 配置接口描述　(6) 设置为路由接口　(7) 192.168.101.1　255.255.255.0

(8) 禁止 DNS 查询　(9) 192.168.101.2　255.255.255.0

(10) 192.168.10.1　255.255.255.0　(11) vlan 10

【问题 3】

(12) 进入编号为 10 的通道接口　(13) 192.168.102.1　255.255.255.0

(14) 配置通道组 10 的模式为启动　(15) 192.168.102.2　255.255.255.0

(16) ip route 0.0.0.0　0.0.0.0　192.168.102.1　(17) ip routing　(18) end

【问题 4】

(19) 启动 DCHP 监听功能　(20) 设置端口为信任端口

解析：

【问题 1】

以太通道可以增加带宽，同时也可以起到负载均衡和冗余备份的作用。

Cisco 的以太通道的协议是 PAgP，IEEE 802.3ad 的以太通道协议是 LACP。

【问题 2】

(5) Switch-core(config-if)#description wgsw-g0/1　　// 配置端口描述

(6) Switch-core(config-if)#no switchport　　// 设置为路由(三层)接口

(7) Switch-core(config-if)#ip address 192.168.101.1 255.255.255.0

(8) Switch1(config)#no ip domain lookup　　// 禁止 DNS 查询

(9) Switch1(config-if)#ip address 192.168.101.2 255.255.255.0

//通过表中可得出 Switch1 的 g0/2 的 IP 地址

(10) Switch1(config-if)#ip address 192.168.10.1 255.255.255.0

//通过图中网管主机的网关地址可得出

(11) Switch1(config-if-range)#switchport access vlan 10　　//设置端口所属的 VLAN

【问题 3】

(12) Switch-core(config)#interface port-channel 10　　// 进入编号为 10 的以太网通道接口

(13) Switch-core(config-if)#ip address 192.168.102.1 255.255.255.0　　//通过表得出 IP 地址

(14) Switch-core(config-if_range)#channel-group 10 mode on　　//分配接口并指定为 PAgp 模式

(15) Switch-core(config-if)#no address 192.168.102.2 255.255.255.0

(16) Switch4(config)#ip route 0.0.0.0 0.0.0.0 192.168.102.1　　//配置默认路由

(17) Switch4(config)# ip routing　　//开启该交换机的三层路由功能

(18) Switch4(config-if-range)#end　　//退回到特权模式

【问题 4】

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP-Snooping 后，会对 DHCP 报文进行侦听，可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，DHCP-Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址。

2.3 本章小结

本章知识点在 2014 年的新大纲中变化较小，只是一些表述方式的调整。

本章主要要求考生掌握交换机的基本配置以及 VLAN 的实施，包括 STP 和 VTP 等。

本章内容为下午科目的重点内容，尤其是 VLAN，基本为每次考试的必考内容，希望考生重点掌握。其中多数会涉及 STP 和 VTP 的相关配置。

第 3 章　路由器与网络互联

大纲要求：

- 路由器的配置，包括命令行接口配置、使用 Web 方式访问路由器、VoIP 配置、路由协议的配置、广域联网、DTP、STP 和 RSTP。
- 远程访问服务器，包括功能和机制。
- 网络接入与服务，包括 HFC、ADSL、FTTx + LAN、WLAN、移动通信、服务供应商、因特网广播、电子商务、电子政务、主机服务提供者和数据中心。
- IP 路由器功能和控制。

3.1　IP 地址与划分

3.1.1　考点辅导

3.1.1.1　IP 地址的分类

IP 地址格式使用的是点分十进制表示法。它包含 32 位，分为 4 个部分，每个部分都是用 8 位二进制字节的十进制表示。一个 IP 地址的 8 位二进制字节格式如 10000001.00000101.00001010.01100100，转换为十进制就是 129.5.10.100。地址的一部分是网络标识符(Net_ID，网络 ID)，另一部分是主机标识符(Host_ID，主机 ID)。

IP 地址共有 5 类：A 类、B 类、C 类、D 类和 E 类。在不同类型的网络中使用不同的 IP 地址类。地址分类反映了网络的大小以及包是单点传送的还是多点传送的。

A 类、B 类和 C 类地址计划用于单点编址方法，但它们用于不同大小的网络。A 类地址用于最大型的网络，该网络的节点数可达 16 777 216 个，在最前 8 位(第一字节)上由 1～126 的值来标识。网络 ID 为前 8 位(第一字节)，主机 ID 为后 24 位(第二、三、四字节)。B 类地址是用于中型网络的单点编址格式，节点数可达 65 536 个，在最前 8 位(第一字节)上由 127～191 的值来标识。网络 ID 为前两个 8 位(第一、二字节)，主机 ID 为后两个 8 位(第三、四字节)。C 类地址是用于 256 个节点以下的小型网络的单点网络通信。最前面的 8 位(第一字节)转换为十进制是在 192～223，网络 ID 为前 24 位(第一、二、三字节)，而主机 ID 为最后 8 位(第四字节)。

D 类地址并不反映网络的大小，只反映通信是多点传送的，所以通常也称为组播。它的四个 8 位字节用来指定其所分配到的接收多点传送的节点组，这个节点组是由多点传送订阅成员组成的。D 类地址的范围为 224.0.0.0～239.255.255.255。

E 类地址用于试验，地址的第一个 8 位字节的范围为 240～255。

除了这些用于分类编址的 IP 地址外，还有一些具有特殊目的的 IP 地址，如 255.255.255.255，这是发送到所有网络位置的广播地址。以 127 作为第一个 8 位字节开始的

数据包用于网络测试。对于一个完整的网络，只需提供网络 ID 号，将其他字节均设置为 0 便可指定。例如：B 类地址网络 132.155.0.0 和 C 类地址网络 220.127.10.0，都指定的是完整的网络。

根据用途和安全性级别的不同，还可以将 IP 地址分为两类：公共地址和私有地址。公共地址在 Internet 中使用，它可以在 Internet 中随意访问；私有地址只能在内部网络中使用，只有通过代理服务器才能与 Internet 通信。

一个机构或网络要连入 Internet，必须要申请公共 IP 地址。但是考虑到网络安全和内部实验等特殊情况，IP 地址中专门保留了三个区域作为私有地址，其地址范围如下。

10.0.0.0/8：10.0.0.0～10.255.255.255。

172.16.0.0/12：172.16.0.0～172.31.255.255。

192.168.0.0/16：192.168.0.0～192.168.255.255。

使用保留地址的网络只能在内部进行通信，而不能与其他网络互联。因为本网络中的保留地址同样也可能被其他网络使用，如果进行网络互联，那么在寻找路由时就会因为地址的不唯一而出现问题。但是这些使用保留地址的网络可以通过将本网络内的保留地址转换成公共地址的方式来实现与外部网络的互联，这里需要使用网络地址转换技术。

3.1.1.2　子网掩码

编址的另一个特殊形式是子网掩码。子网掩码的目的有两个：一是显示使用的编址类别，二是将网络分成子网来控制网络流量。在第一种情况下，子网掩码可使得应用程序能够确定 IP 地址的哪一部分是表示网络 ID，哪一部分是表示主机 ID。例如，一个 A 类地址网络的默认子网掩码是第一个 8 位字节均为二进制的 1，其他字节均为二进制的 0：11111111.00000000.00000000.00000000(255.0.0.0)。

如果要将网络分成子网，子网掩码应包含子网 ID，这个子网 ID 是由网络管理员决定的，存在于网络 ID 和主机 ID 之内。例如，可以指定 B 类地址的整个第三个 8 位字节来说明子网 ID，如 11111111.11111111.11111111.00000000(255.255.255.0)；另一种选择是只指定第三个 8 位字节的前 5 位作为子网 ID，后 3 位和余下的 8 位字节用于指定主机 ID，如 11111111.11111111.11111000.00000000(255.255.248.0)。

使用子网掩码将网络分成一系列小型网络，可以使得第三层设备能够有效地忽略传统的地址分类命名，因此在通过多个子网和额外的网络地址将网络进行分段时就有了更多的选项，克服了四个 8 位字节长度的限制。同样是利用子网掩码工具，1992 年出现了一种新的忽略地址分类命名的方法，它是无分类域间路由(Classless Inter-Domain Routing，CIDR)编址方法。

引入 CIDR 后，意味着网络“类”(比如 A 类地址、B 类地址等)的概念已经被取消，取而代之的是“网络前缀”的概念。CIDR 的基本思想是取消地址的分类结构，允许以可变长分界的方式分配网络数。它支持路由聚合，可限制 Internet 主干路由器中必要路由信息的增长。

CIDR 编址的方法是在点分隔的十进制符号之后画一个斜杠“/”，并在斜杠后加上子网掩码“1”的总个数。比如 202.102.0.0/23。我们知道，202.102.0.0 是 C 类网络地址(默认是 24 位子网掩码)；而采用 CIDR 编址后，202.102.0.0/23(23 位子网掩码)既不属于 C 类网络地

址，也不属于 B 类网络地址。但是，网络地址 202.102.0.0/23 提供了更多的信息节点(510 个)，而默认的 C 类网络地址 202.102.0.0 只提供了 254 个信息节点。

可见，CIDR 编址方法为中型的网络提供了更多的 IP 地址选项。例如，对于需要 262 144 个节点的网络，其 CIDR 网络编址方案可以是 165.100.0.0/14。

3.1.1.3 IPv6

到目前为止 IPv4 已经存在 20 多个年头了。在 20 世纪 90 年代中期，人们就认识到了它的局限性，主要的一点是 32 位地址太有限。在当前的网络使用状况下，IPv4 所有的地址很快将会消耗尽。

另外，由于 IPv4 不能提供网络安全，也不能实施复杂的路由选项(如在 QoS 的水平上创建子网等)，所以它的应用也受到了限制。同时，IPv4 除了能提供广播和多点传送编址外，并不具备用多个选项来处理多种不同的多媒体应用程序(如流式视频或视频会议等)。

为了适应 IP 的爆炸式应用，Internet 工程任务组(IETF)开始了 IPng(IP next generation)的初步开发。1996 年，通过对 IPng 的研究诞生了一种称为 IPv6 的新标准，并在 RFC 1883 中得到定义。IPv6 的目的是从 IPv4 中提供一条逻辑的增长路径，使得应用程序和网络设备可以处理新出现的要求。目前，虽然 IPv4 仍应用在全世界的绝大多数网络中，但向 IPv6 的升级已经开始了。IPv6 的新特点如下。

- 具有 128 位编址能力。
- 一个单独的地址对应着多个接口。
- 地址自动配置并可用 CIDR 编址。
- 以 40 字节的头取代了 IPv4 的 20 字节的头。
- 可将新的 IP 扩展的头用于特殊需要，包括用于更多的路由技术和安全选项中。

IPv6 编址使得一个 IP 标识符可以与多个不同的接口相关，从而可以更好地处理多媒体信息流量。在 IPv6 网络中，多媒体流量不是通过广播或多点传送，而是将所有接收接口都指定为同一个地址传送。

IPv6 并不沿基于分类的地址而行，而是与 CIDR 兼容的，从而其地址可以通过很大范围的选项来进行配置，并使得路由和子网的通信更出色。同时，它还提供了多种选项，使得我们可以在一个组织内、一个单独的地址内，根据地理位置、组织及类型的不同来创建各异的网络。IPv6 的编址是自动配置的，可以减轻网络管理员管理和配置地址的工作负荷。它支持两种自动配置技术：一种是基于动态主机配置协议(DHCP)，另一种是基于无状态的自动配置技术。在无状态自动配置中，网络设备自己指派 IP 地址，而不是从服务器中获得。它通过简单地将 NIC 的 MAC 地址与从子网路由器中获得的子网命名结合在一起来创建地址。

IPv6 数据包的传送类型分为单点传送、任意点传送和多点传送。在单点传送包中，一个单独的网卡接口对应一个单独的地址，并且是点到点传输的。任意点传送的包中包含着与多个接口关联的目标地址，而且这些接口通常位于不同的节点上。任意点传送的包只向最近的接口传送，并不试图到达具有同一地址的其他接口。多点传送包与任意点传送包相似，也具有与多个接口相关联的目标地址，但是与任意点传送包不同的是，多点传送包将流向具有这个地址的所有接口。

1. 头部格式

如图 3-1 所示，基本的 IPv6 头包含以下域。

- 版本：这是版本标识符，它的值为 6。
- 流量分类：该域说明了一个包是否包含着协助控制网络阻塞的信息。用于阻塞控制的包可以提供诸如过滤、自动 E-mail 投递和与 Internet 相关的控制等特征。不控制阻塞的包是携带数据的，可以指定不同的优先级来说明丢弃一个包对信息的影响。例如，携带声频的包的优先级应当设置得高一些，以此说明一定要避免丢弃包，因为这样会干扰声音播放的连续性。
- 流标签：此处的信息用于向路由器说明包需要以特殊的方法来进行处理。例如，多点传送包需要额外的网络资源，而秘密的包需要更高的安全性。
- 有效负载长度：该域说明了包有效负载的大小(不计包的头)。
- 下一个头：由于可以添加扩展的头，所以当基本的头到了结尾时，该域就提供了有关预期的头是何种类型的信息。如果没有包含扩展的头，那么下一个头就是 TCP 或者 UDP。
- 跳数限制：该域用来对 IPv4 TTL 域进行修正。当创建好一个包后，就会在跳数限制(Hop Limit)域中输入最大的路由器跳数值，包每次经过第三层设备时，该值都会减 1。当第三层设备遇到的包的跳数限制为 0 时，就将该包丢弃，以免在网络上不断地传播。
- 源地址：这是指发送设备的 128 位地址。
- 目标地址：此域包含着接收包设备的 128 位地址。

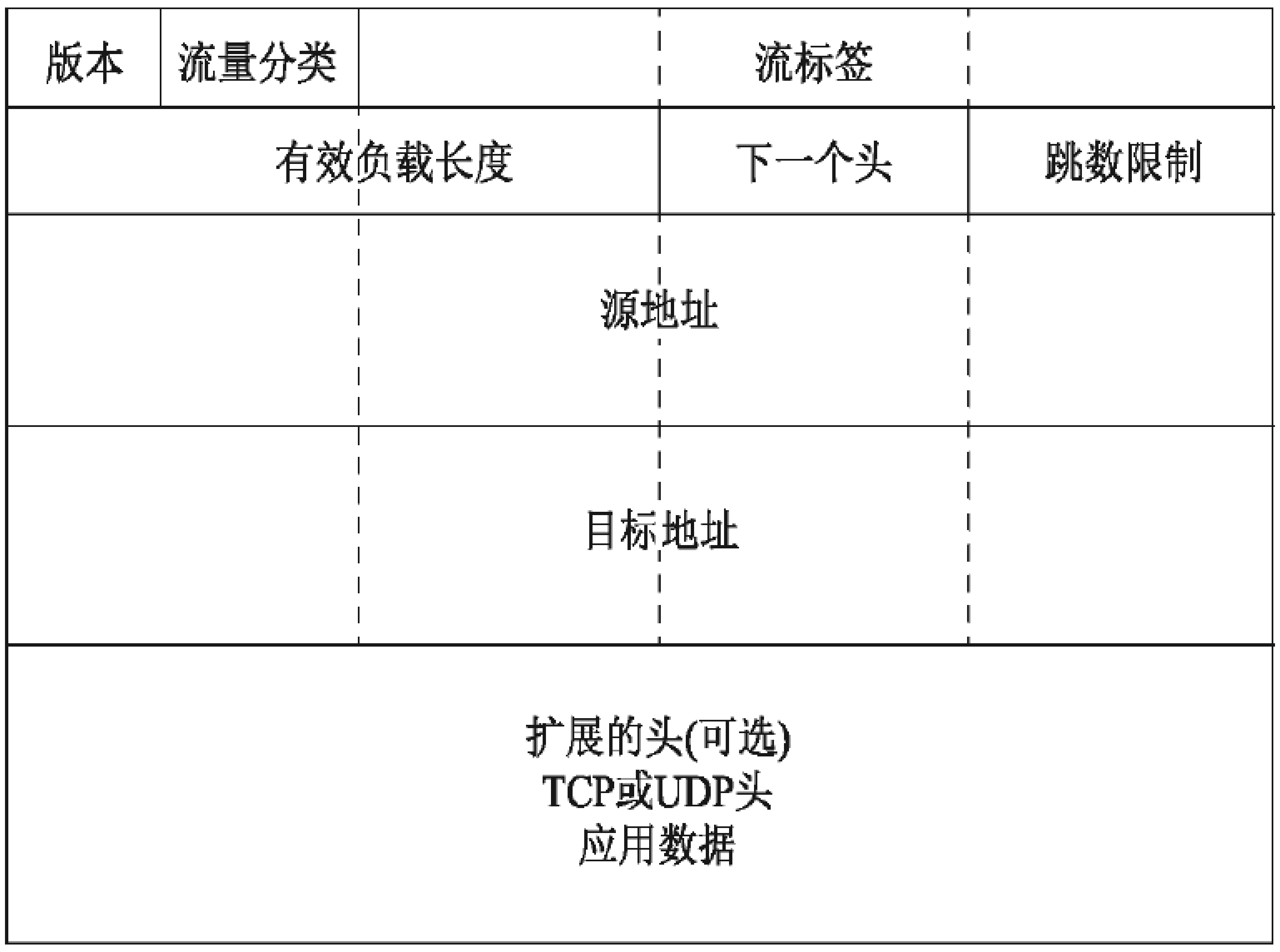


图 3-1　IPv6 数据包

2. IPv6 扩展头部及其功能

当前，IPv6 定义了下列 6 种扩展头。

- 步跳扩展头。
- 路由扩展头。

- ◆ 分段扩展头。
- ◆ 验证扩展头。
- ◆ 安全负载封装扩展头。
- ◆ 目标选项扩展头。

IPv6 的主头必须出现在所有的扩展头之前。扩展头是可选的，可以组合使用，也可以一个都不用。在单个的包中，每种类型的扩展头只能出现一次。当同时使用多个扩展头时，它们必须严格遵守上面列举的顺序。例如，如果同时使用了路由扩展头、验证扩展头和安全负载封装扩展头，那么包头的域必须按照如下的顺序出现：①IPv6 的主头；②路由扩展头；③验证扩展头；④安全负载封装扩展头；⑤TCP 或 UDP 头；⑥应用数据，如图 3-2 所示。在每一个扩展头中，第一个字节为一个 8 位的“下一个头(Next Header)”字段，该字段用以指明后面紧跟的是哪个头。在最后一个扩展头中，“下一个头”域包含的值为 59，表明该扩展头是最后一个。在上面的例子中，路由扩展头中的“下一个头”域指出后面紧跟的是验证扩展头；验证扩展头的“下一个头”域指出后面紧跟的是安全负载封装扩展头。除分段扩展头之外，在“下一个头”域后面紧跟着的是一个 8 位的“头扩展长度”域，用以指明该扩展头的长度。每个扩展头的长度必须为 8 的倍数个字节。

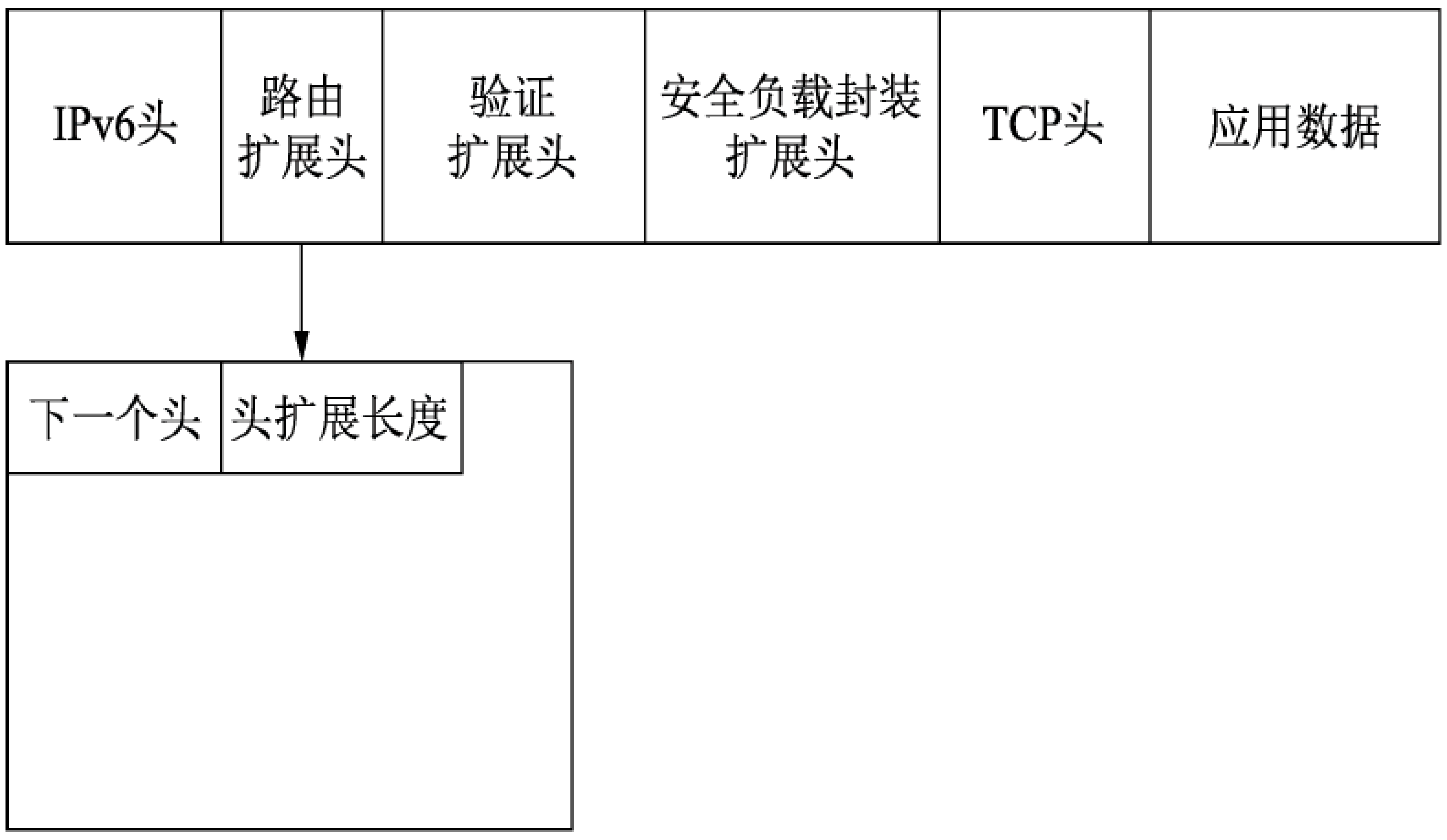


图 3-2 IPv6 数据包扩展头

步跳扩展头用于大数据的传输，例如多媒体视频数据包。其应用数据负载可以从 65 535 字节到 4 亿字节。数据包所经过的每一个路由都将读取步跳扩展头，这样会略微增加路由器的处理延迟。

路由扩展头使用按顺序排列的路由地址来标识整个路由，用户可以通过配置该头达到让包沿相同路径传输的目的。这种包可用于某些特殊的情况，例如当某条路径上的路由器出现故障的时候。

在 IPv6 中，每个发送节点通过使用搜索包，运行一个最大传输单元(MTU)路径发现的过程，便可以确定接收网络所允许的最大包尺寸。该路径发现产生的信息包括是否有某个路由器出现故障和目标网络是否需要较小的包(IPv6 包最多可以包括 1280 个 8 位字节)。当向使用小于 1280 个 8 位字节包的网络上发送包时，IPv6 便对包进行分段。根据 MTU 路径发现所获取的信息，发送节点将数据包进行分段，在包头中添加分段扩展头，告知接收者包是如何分段的。将数据包分段的能力在从以太网向令牌环网发送包或者在具有不同大小

包的快速以太网和千兆以太网之间传输数据时尤为重要。当把一个包进行分段后，每一个段都分配到了一个分段组内的标识符(每组是唯一的)，该标识符含有 32 位标识符域，这样在接收数据的时候，不同组的分段就可以很容易地被区分开。

验证扩展头可用于确认数据包的完整性(IP 头、TCP 头和数据)，即保证接收到的数据包和发送的数据包是一致的。每一个扩展头的每一个域以及负载数据都需要进行验证。如果在数据包发出后某个域中的值有所改动(对于步跳计数来说肯定要发生变化，因此步跳计数除外)，该字域的验证值则为 0。通常，验证扩展头和安全负载封装扩展头是一起使用的，这样便可以对包进行验证和加密/解密。当使用这两个扩展头时，在接收节点上将做如下处理。

(1) 首先验证 IP 头，然后验证 TCP 头(如果 IP 头或者 TCP 头被加密，则首先需要进行解密)。

(2) 在验证之后，使用安全负载封装扩展头中的信息对负载进行解密。

(3) 在解密了负载后，对负载进行验证。

在有安全需求的网络上，可以使用安全负载封装扩展头对 IP 包负载或者 TCP/IP 头负载进行加密，该扩展头支持与数据加密标准(DES)相兼容的密钥加密技术。

3.1.2 典型例题分析

【说明】(2017 年下半年下午试题四)

某公司网络拓扑图如图 3-3 所示。

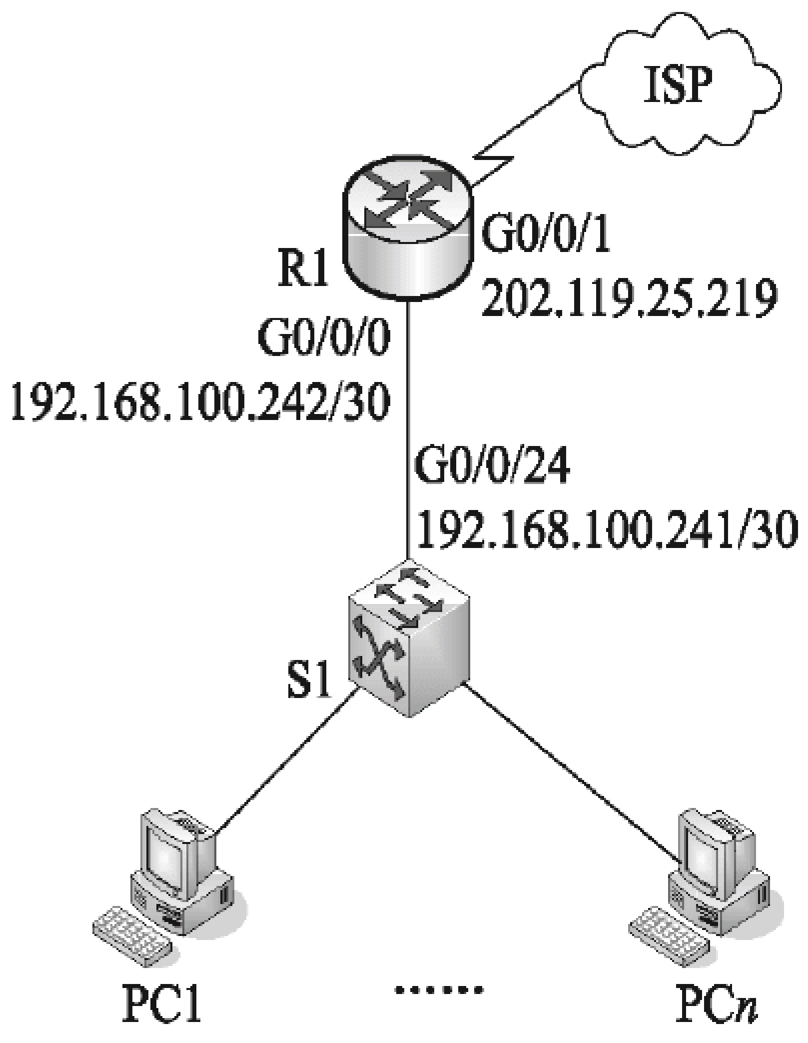


图 3-3 某公司网络拓扑图

【问题 1】(5 分)

为了便于管理公司网络，管理员根据不同部门对公司网络划分了 VLAN，VLAN 编号及 IP 地址规划如表 3-1 所示。考虑到公司以后的发展，每个部门的 IP 地址规划均留出了一定的余量。请根据需求，将表 3-1 补充完整。

表 3-1　VLAN 编号及 IP 地址规划

部　门	VLAN 编号	主机数量	IP 地址范围	子网掩码
行政部门	VLAN100	32	192.168.100.129～____(1)____	____(2)____
营销部门	VLAN105	68	192.168.100.1～192.168.100.126	255.255.255.128
财务部门	VLAN110	8	192.168.100.193～192.168.100.222	____(3)____
后勤部门	VLAN115	8	____(4)____～192.168.100.238	255.255.255.240

公司计划使用 24 接口的二层交换机作为接入层交换机，根据以上主机数量在不考虑地理位置的情况下，最少需要购置____(5)____台接入层交换机。

【问题 2】(10 分)

公司申请了 14 个公网 IP 地址，地址范围为 202.119.25.209～202.119.25.222。其中，202.119.25.218～202.119.25.222 作为服务器和接口地址保留，其他公网 IP 地址用于公司访问 Internet。公司使用 PAT 为营销部门提供互联网访问服务。请根据描述，将下面配置代码补充完整。

```
<Huawei>system-view
[Huawei]____(6)____R1
[R1]user-interface____(7)____//进入 console 用户界面视图
[R1-ui-console0]authentication-mode____(8)____
Please configure the login password (maximum length 16): huawei
[R1-ui-console0]quit
[R1]int GigabitEthernet, 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.100.242 255.255.255.252
[R1-GigabitEthernet0/0/0]____(9)____
[R1]____(10)____2000
[R1-acl-2000]____(11)____5 permit source 192.168.100.0____(12)____
[R1-acl-basic-2000]quit
[R1]nat address-group 1____(13)____202.119.25.217
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet 0/0/1]ip address____(14)____255.255.255.240
[R1-GigabitEthernet 0/0/1]____(15)____outbound 2000 address-group1
[R1]rip
[R1-rip-1]version 2
[R1-rip-1]network 192.168.100.0
交换机配置略……
```

答案：

【问题 1】

(1) 192.168.100.190　(2) 255.255.255.192　(3) 255.255.255.240

(4) 192.168.100.225　(5) 5

【问题 2】

(6) sysname (7) console 0 (8) password (9) quit (10) acl (11) rule (12) 0.0.0.255 (13) 202.119.25.209 (14) 202.119.25.219 (15) NAT

解析：

【问题 1】由图形说明可知，行政部需要 32 个有效主机地址，因此分配主机位位数为 6，网络号位数则为 26，对应子网掩码为 255.255.255.192，对应的网段为 192.168.100.128，最后一个有效 IP 地址为 192.168.100.1011 1110 即 192.168.100.190。同理可求得其他部门的 IP 及子网掩码。

主机数量一共有 32+68+8+8=116 台，不考虑位置，则需要接入交换机(24 接口) 116/24=4.8(台)，至少需要 5 台交换机。

【问题 2】[Huawei] sysname R1 表示配置设备名为 R1。

[R1] user-interface console 0 表示进入 Console 用户界面视图，参数 interface-number 用来指定 Console 口编号，只能为 0。

登录 Console 用户界面的验证方式。当用户通过 Console 口登录交换机时终端会提示输入登录密码，登录交换机。使用 quit 命令可以退出当前模式，空(10)[R1] acl 2000 语句定义了一个标准 ACL 2000。

[R1-acl-2000] rule 5 permit source 192.168.100.0 0.0.0.255，该语句表明允许源地址为 192.168.100.1～192.168.100.254 的数据包通过，其中由 192.168.100.0/24 可得子网掩码是 255.255.255.0，而 ACL 的子网掩码用反向子网掩码即 0.0.0.255。

空(13)所在语句意义为配置 IP 地址池 1，包括两个公网地址 202.119.25.209 和 202.119.25.217。

[R1] interface GigabitEthernet 0/0/1

[R1-GigabitEthernet 0/0/1] ip address 202.119.25.219 255.255.255.240

[R1-GigabitEthernet 0/0/1] nat outbound 2000 address-group1

此处语句的意义为在出接口 GigabitEthernet 0/0/1 上配置 ACL 2000 与 IP 地址池 1 相关联。

3.1.3 同步练习

1. IPv6 将 IP 地址空间从 __(1)__ 位扩展到 __(2)__ 位。

2. 子网掩码为 255.255.255.0 代表什么意义？

3. 单位分配到一个 B 类的 IP 地址，其 Net_ID 为 172.250.0.0。该单位有 4000 台机器，分布在 16 个不同的地点。请分析：

(1) 选用子网掩码为 255.255.255.0 是否适合；

(2) 给每一个地点分配一个子网号码，算出每个主机号码的最小值和最大值。

3.1.4 同步练习参考答案

1. **答案：**

(1) 32　　　(2) 128

2. **答案：**

若是 A 类网络的子网掩码，则前 8 位为网络号，中间 16 位为子网号，最后 8 位为主机号；若是 B 类网络，则前 16 位为网络号，中间 8 位为子网号，最后 8 位为主机号；若是 C

类网络，则为 C 类网络的默认子网掩码。

3. 答案：

(1) 选用子网掩码为 255.255.255.0，子网位有 8 位，每个子网最多有 254 台主机($2^8-2=254$)。如果 4000 台机器是平均分配的，则 4000÷16=250(台)——不超过 254 台，选用这个子网掩码是合适的；如果不是平均分配，当某个子网主机数目超过了 254 台，选用这个子网掩码是不合适的。

(2) 如果还是选用 255.255.255.0 作为子网掩码，每个子网中主机号为 0.0.0.1～0.0.0.254。

3.2　路由器的配置与网络互联

3.2.1　考点辅导

3.2.1.1　路由器的功能

近几年来，基于 TCP/IP 协议的 Internet 已逐步发展成为当今世界上规模最大、拥有用户和资源最多的一个超大型计算机网络，TCP/IP 协议也因此成为事实上的工业标准。IP 网络正逐步成为当代乃至未来计算机网络的主流。路由器作为 IP 网络的核心设备，将不同的 IP 子网互联起来构成一个规模巨大的 IP 网络。

路由器是工作在 OSI 标准模型的第三层——网络层的数据包转发设备，它通过转发数据包来实现网络互联。虽然路由器可以支持多种协议(如 TCP/IP、IPX/SPX 和 Apple Talk 等协议)，但是在我国绝大多数路由器上运行 TCP/IP 协议。路由器通常连接两个或多个由 IP 子网或点到点协议标识的逻辑端口，至少拥有 1 个物理端口。路由器根据收到的数据包中网络层地址以及路由器内部维护的路由表来决定输出的端口以及下一跳地址，并且通过重写链路层数据包头，实现转发数据包。路由器通过动态维护路由表来反映当前的网络拓扑，并通过与网络上其他路由器交换路由和链路信息来维护路由表。

作为网络的核心设备，路由器应该具备以下功能。

- ◆ 接口功能：该功能负责将路由器连接到网络。路由器的接口可分为局域网接口和广域网接口两种。局域网接口主要包括以太网、令牌环、令牌总线和 FDDI 等网络接口。广域网接口主要包括 E1/T1、E3/T3、DS3、通用串行口(可转换成 X.21 DTE/DCE、V.35 DTE/DCE、RS232 DTE/DCE、RS449 DTE/DCE 和 EIA530 DTE)等网络接口。
- ◆ 通信协议功能：该功能负责处理通信协议，可以包括 TCP/IP、PPP、X.25、帧中继等协议。
- ◆ 数据包转发功能：该功能主要负责按照路由表中的内容在各端口(包括逻辑端口)间转发数据包并且改写链路层数据包头信息。
- ◆ 路由信息维护功能：该功能负责运行路由协议并维护路由表。路由协议可包括 RIP、EIGRP、OSPF、ISIS、BGP 等协议。
- ◆ 管理控制功能：该功能可再细分为 SNMP 代理功能、Telnet(SSH)服务功能、本地管理、远端监控和 RMON(MIB)5 个功能。通过这 5 种不同的功能可以对路由器进

行控制管理，并且允许路由器记录日志。

- 安全功能：该功能用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙以及地址分配等。

3.2.1.2 路由器的配置

1. 路由器的命令状态

与交换机的配置类似，路由器的配置操作有 3 种模式，即用户视图、系统视图和具体业务视图。用户视图模式下，在用户视图下，用户可以完成查看运行状态和统计信息等功能，这些命令对路由器的正常工作没有影响；在系统视图模式下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图；在具体业务视图模式下，用户可以配置接口相关的物理属性、链接层特性及 IP 地址等重要参数，路由协议的大部分参数也需要在这种模式下配置。

其中，配置模式又分为全局配置模式、接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

<Switch>。在交换机正常启动后，用户使用终端仿真软件或 Telent 登录交换机，可自动进入用户配置模式，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

[Switch]。路由器处于系统视图命令状态，在<Switch>提示符下输入 system-view，可进入系统视图状态，这时不仅可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

[Switch-vlan]。路由器处于具体的业务视图状态，在[Switch]提示符下输入需要配置的业务命令，可进入该状态。退出具体的业务输入 quit。

在开机自检时，按 Ctrl+Break 组合键可进入 BootROM menu 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导，或者进行路由器口令恢复时要进入该状态。

2. 路由器的基本配置

配置 enable 口令、enable 密码和主机名，在路由器中同样可以配置启用口令(enable password)和启用密码(enable secret)，一般情况下只需配置一个就可以，当两者同时配置时，后者生效。这两者的区别是启用口令以明文显示而启用密码以密文形式显示。主机名及路由器口令的设置和上一节对交换机配置的主机名及口令相同，这里不再赘述。

配置路由器以太网接口，路由器一般提供一个或多个以太网接口槽，每个槽上会有一个以上以太网接口。以太网接口因此而命名为{Ethernet 槽位/端口}或{GigabitEthernet 槽位/端口}，例如 Ethernet0/0、GigabitEthernet0/0/1，也可缩写为 Eth0/0、GE0/0/1。

对以太网接口做如下配置：

```
#设置系统的日期、时间和时区
<Huawei>clock timezone BJ add 08:00:00
<Huawei>clock datetime 20:10:00 2015-03-26

#设置设备名称和管理 IP 地址
<Huawei>system-view
[Huawei]sysname Server
```

```
[Server]interface gigabitethernet 0/0/0
[Server-GigabitEthernet0/0/0]ip address 10.137.217.177 24
[Server-GigabitEthernet0/0/0]quit

#设置 Telnet 用户的级别和认证方式
[Server] telent server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4]user privilege level 15
[Server-ui-vty0-4]authentication-mode aaa
[Server-ui-vty0-4]quit
[Server]aaa
[Server-aaa] local-user admin1234 password irreversible-cipher
Helloworld@6789
[Server-aaa] local-user admin1234 privilege level 15
[Server-aaa] local-user admin1234 service-type telent
[Server-aaa]quit
```

由于同一厂商的网络设备往往采用一种网络操作平台，交换机、路由器的配置以及命令的使用都是相似的。

3. 批量配置技术

大型网络的组网和网络管理中都会同时用到多个路由器和交换设备，可以通过批量配置技术快速配置多台网络设备。例如，华为交换机 AR 系列路由器通过 Auto-Config 功能实现设备的批量配置，Auto-Config 是指新出厂或空配置设备加电启动时采用的一种自动加载版本文件(包括系统软件、补丁文件、配置文件)的功能。

如图 3-4 所示，RouterA、RouterB 和 RouterC 运行 Auto-Config 功能后，设备作为 DHCP 客户端定时向 DHCP 服务器发送 DHCP 请求报文以获得配置信息，然后 DHCP 服务器向待配置设备响应 DHCP 应答报文，报文内容包括分配给待配置设备的 IP 地址、文件服务器的 IP 地址、文件服务器的登录方式、版本文件的配置信息(此信息也可以通过中间文件获取，中间文件需要预先编辑存放在文件服务器)，最后设备根据收到的 DHCP 响应报文中携带的配置信息向指定的文件服务器自动获取版本文件并设置为下次启动加载的文件，待设备重启后，设备就实现了版本文件的自动加载。

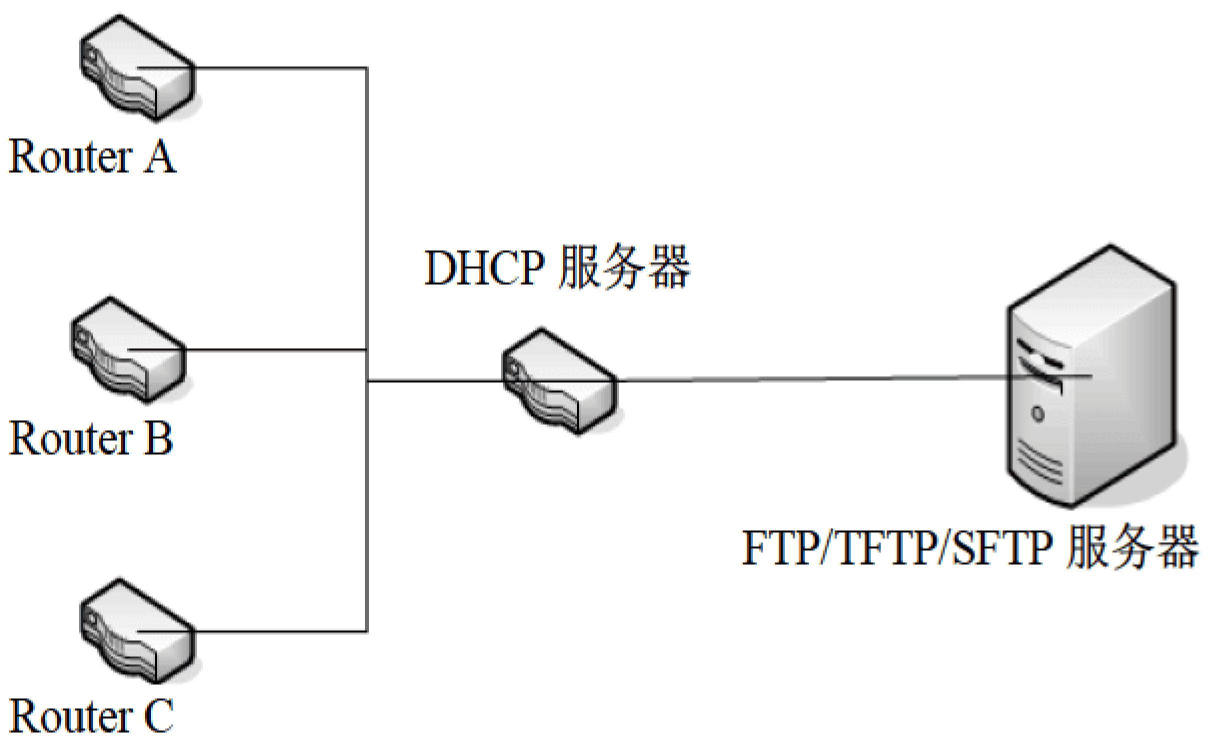


图 3-4　DHCP 服务器发送请求

若网络中有一台 SFTP 服务器(GE0/0/1，IP 地址 172.16.100.100/24)，一台 DHCP 服务器(GE0/0/1，IP 地址 172.16.100.1/24 用于与 SFTP 互联；Eth1/0/1-3，VLANIF10，IP 地址 172.16.200.100/24 用于与待配置路由器互联)，3 台待配置路由器。举例说明配置同网段 Auto-Config 步骤。

步骤 1：配置 SFTP 服务器。

```
#配置 SFTP 服务器功能及参数
<Huawei> system-view
[Huawei] sysname SFTP Server
[SFTP Server] rsa local-key-pair create The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512～2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential secunty risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys…
…………………………………………………………………….
[SFTP Server] sftp server enable

#配置 SSH 用户登录的用户界面
[SFTP Server] user-interface vty 0 4
[SFTP Server-ui-vty0-4] authentication-mode aaa
[SFTP Server-ui-vty0-4] protocol inbound all
[SFTP Server-ui-vty0-4] user privilege level 15
[SFTP Server-ui-vty0-4] quit

#配置 SSH 用户
[SFTP Server] aaa
[SFTP Server-aaa] local-user user password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters,
including lowercase letters, uppercase letters, numerals and special
characters.
Please entes password:
Please confirm password:
[SFTP Server-aaa] local-user user privilege level 15
[SFTP Server-aaa] local-user user service-type ssh
[SFTP Server-aaa] local-user user ftp-directory flash:\autoconfig
[SFTP Server-aaa] quit
[SFTP Server] ssh user user authentication-type password

#配置 SFTP 服务器的 IP 地址
[SFTP Server] interface gigabitethernet 0/0/1
[SFTP Server-GigabitEthernet0/0/1] ip address 172.16.100.100 255.255.255.0
[SFTP Server-GigabitEthernet0/0/1 quit

#在 SFTP 服务器上配置缺省路由
[SFTP Server] ip route-static 0.0.0.0 0.0.0.0 172.16.100.1
```

步骤 2：将配置文件、系统软件和补丁文件上传至 SFTP 服务器的工作目录 flash:\autoconfig 上(上传步骤略)。

步骤 3：配置 DHCP 服务器(以 AR2220 为例)。

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] vlan 10
[DHCP Server-vlan10] quit
[DHCP Server] interface ethernet 1/0/1
[DHCP Server-Ethernet1/0/1] port link-type hybrid
[DHCP Server-Ethernet1/0/1] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/1] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/1] quit
[DHCP Server] interface ethernet 1/0/2
[DHCP Server-Ethernet1/0/2] port link-type hybrid
[DHCP Server-Ethernet1/0/2] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/2] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/2] quit
[DHCP Server] interface Ethernet 1/0/3
[DHCP Server-Ethernet1/0/3] port link-type hybrid
[DHCP Server-Ethernet1/0/3] port hybrid untagged vlan 10
[DHCP Server-Ethernet1/0/3] port hybrid pvid vlan 10
[DHCP Server-Ethernet1/0/3] quit
[DHCP Server] interface gigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 172.16.100.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface vlanif 10
[DHCP Server-Vlanif10] ip address 172.16.200.100 255.255.255.0
[DHCP Server-Vlanif10] dhcp select global
[DHCP Server-Vlanif10] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 172.16.200.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 172.16.200.100
[DHCP Server-ip-pool-auto-config] option 67 ascii ar_V200R008
(C20&C30) .cfg
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config] option 142 cipher Huawei@123
[DHCP Server-ip-pool-auto-config] option 143 ip-address 172.16.100.100
[DHCPServer-ip-pool-auto-config]option145ascii vrpfile=auto_V200R008
(C20&C30) .cc;vrpver=V200R008 (C20&C30) ;patchfile=ar_V200R008
(C20&C30) .pat;
[DHCP Server-ip-pool-auto-config] quit
```

步骤 4：待配置设备 RouterA、RouterB 和 RouterC 通电启动，Auto-Config 流程开始运行。

步骤 5：检查配置结果。

Auto-Config 流程结束后，登录到待配置设备，执行命令 display startup，查看设备当

前的启动系统软件，启动配置文件和启动补丁文件。

以 RouterA 为例：

```
<Huawei> display startup
MainBoard:
   Startup system software:          flash:/ar_V200R008 (C20&C30) .cc
   Next startup system sofiware:         flash:/ar_V200R008
(C20&C30) .cc
   Backup system software for next startup:   null
   Startup saved-configuration file:        flash:/ar_V200R008
(C20&C30) .cfg
   Next startup saved-configuration file       flash:/ar_V200R008
(C20&C30) .cfg
   Startup license file:                  null
   Next startup license file:                null
   Startup patch package:                 flash:/ar_V200R008
(C20&C30) .pat
   Next startup patch package:          flash:/ar V200R008 (C20&C30) .pat
   Startup voice-files:                   null
   Next startup voice-files:                 null
```

4. 配置静态路由

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径，网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

1) IPv4 静态路由设置

在创建静态路由时，用户可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

◆ 对于点到点接口，指定出接口。

◆ 对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。

◆ 对于广播接口(如以太网接口)，指定下一跳。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。

操作步骤如下。

(1) 执行命令 system-view，进入系统视图。

(2) 配置 IPv4 静态路由。

◆ 在公网上配置 IPv4 静态路由：ip route-static ip-address { mask | mask-length } { nexthop-address | interface-type interface-number [nexthop-address] | vpn-instance vpn-instance-name nexthop-address } [preference preference | tag tag] * [description text]

◆ 在 VPN 实例中配置 IPv4 静态路由：ip route-static vpn-instance vpn-source-name destination-address { mask | mask-length } { nexthop-address [public] | interface-type

interface-number [nexthop-address] | vpn-instance vpn-instance-name nexthop-address } [preference preference | tag tag] * [description text]

2)　IPv6 静态路由设置

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

- ◆　对于点到点接口，指定出接口。
- ◆　对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。
- ◆　对于广播类型接口，指定出接口。如果也指定下一跳，下一跳地址可以不是链路本地地址。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv6 静态缺省路由。缺省情况下，没有创建 IPv6 静态缺省路由。

操作步骤如下。

(1)　执行命令 system-view，进入系统视图。

(2)　配置 IPv6 静态路由。

- ◆　在公网上配置 IPv6 静态路由：ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-number [nexthop-ipv6-address] | nexthop-ipv6-address } [preference preference | tag tag] * [description text]
- ◆　在 VPN 实例中配置 IPv6 静态路由：ipv6 route-static vpn-instance vpn-instance-name dest-ipv6-address prefix-length { [interface-type interface-number] nexthop-ipv6-address | nexthop-ipv6-address [public] | vpn-instance vpn-destination-name nexthop-ipv6-address } [preference preference | tag tag] * [description text]

3.2.1.3　配置路由协议

1. 配置 RIP 协议

1) 配置 RIP 协议

RIP 是距离矢量路由选择协议的一种。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到了全网。

RIP 使用非常广泛，它简单、可靠，便于配置。RIP 版本 2 还支持无类域间路由(Classless Inter-Domain Routing, CIDR)、可变长子网掩码(Variable Length Subnetwork Mask, VLSM)和不连续的子网，并且使用组播地址发送路由信息。但是 RIP 只适用于小型的同构网络，因为允许的最大跳数为 15，任何超过 15 个站点的目的地均被标记为不可达。RIP 每隔 30s 广播一次路由信息。

RIP 应用于 OSI 网络七层模型的应用层。各厂家定义的管理距离(AD，即优先级)略有不同，华为定义的优先级是 100。

假设有如图 3-5 所示的网络拓扑结构，试通过配置使 RouterA、RouterB、RouterC 和 RouterD 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。

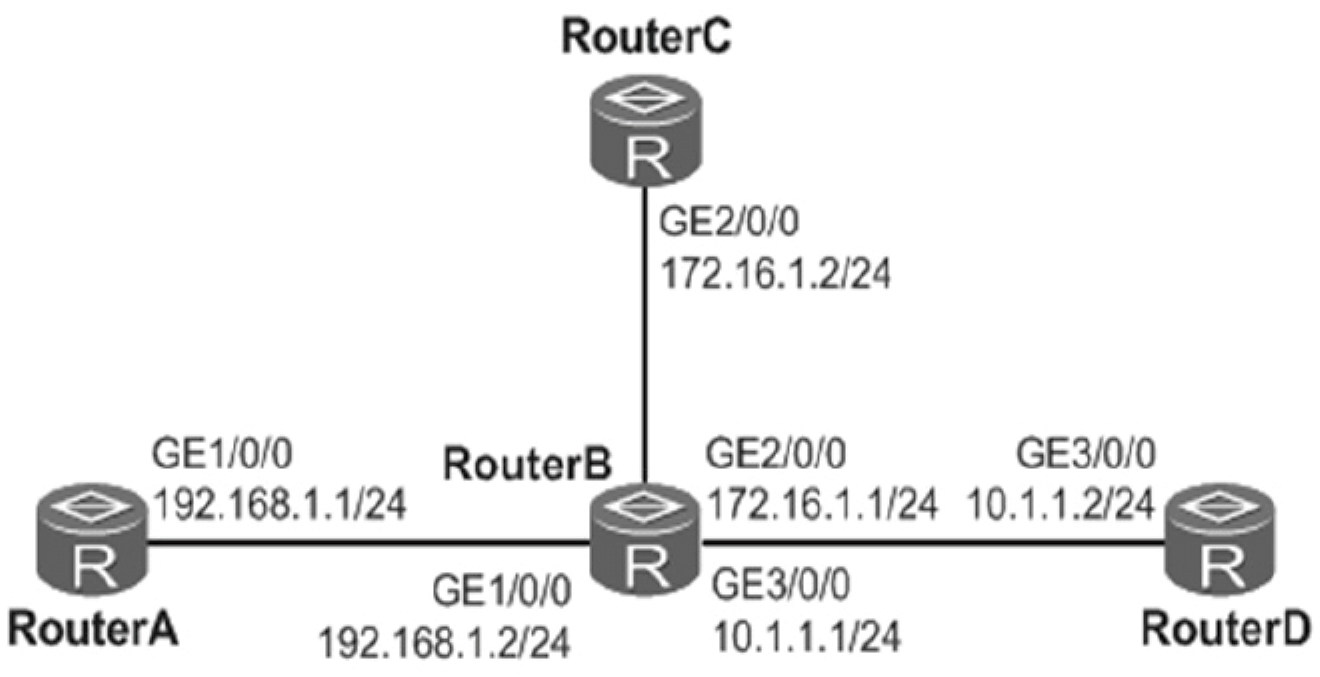


图 3-5　网络拓扑结构

(1) 配置思路。

采用如下的思路配置 RIP 的版本：

◆ 配置各接口的 IP 地址，使网络可达。
◆ 在各路由器上使能 RIP，配置 RIP 基本功能。
◆ 在各路由器上配置 RIP-2 版本，查看精确的子网掩码信息。

(2) 数据准备。

为完成此配置，需准备如下数据：

◆ 在 RouterA 上指定使能 RIP 的网段 192.168.1.0。
◆ 在 RouterB 上指定使能 RIP 的网段 192.168.1.0，172.16.0.0，10.0.0.0。
◆ 在 RouterC 上指定使能 RIP 的网段 172.16.0.0。
◆ 在 RouterD 上指定使能 RIP 的网段 10.0.0.0。
◆ 在 RouterA、RouterB、RouterC 和 RouterD 上配置 RIP-2 版本。

(3) 操作步骤。

① 配置各接口的 IP 地址(略)。

② 配置 RIP 基本功能。

```
# 配置 RouterA
   [RouterA] rip
   [RouterA-rip-1] network 192.168.1.0
   [RouterA-rip-1] quit
# 配置 RouterB
   [RouterB] rip
   [RouterB-rip-1] network 192.168.1.0
   [RouterB-rip-1] network 172.16.0.0
   [RouterB-rip-1] network 10.0.0.0
   [RouterB-rip-1] quit
# 配置 RouterC
   [RouterC] rip
   [RouterC-rip-1] network 172.16.0.0
   [RouterC-rip-1] quit
```

```
# 配置 RouterD
   [RouterD] rip
   [RouterD-rip-1] network 10.0.0.0
   [RouterD-rip-1] quit
# 查看 RouterA 的 RIP 路由表
   [RouterA] display rip 1 route
   Route Flags: R - RIP
            A - Aging, S - Suppressed, G - Garbage-collect
--------------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
      Destination/Mask       Nexthop     Cost  Tag     Flags   Sec
        10.0.0.0/8          192.168.1.2      1    0        RA      14
        172.16.0.0/16        192.168.1.2      1    0        RA      14
```

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

③　配置 RIP 的版本。

```
# 在 RouterA 上配置 RIP-2
   [RouterA] rip
   [RouterA-rip-1] version 2
   [RouterA-rip-1] quit
# 在 RouterB 上配置 RIP-2
   [RouterB] rip
   [RouterB-rip-1] version 2
   [RouterB-rip-1] quit
# 在 RouterC 上配置 RIP-2
   [RouterC] rip
   [RouterC-rip-1] version 2
   [RouterC-rip-1] quit
# 在 RouterD 上配置 RIP-2
   [RouterD] rip
   [RouterD-rip-1] version 2
   [RouterD-rip-1] quit
```

④　验证配置结果。

```
# 查看 RouterA 的 RIP 路由表
   [RouterA] display rip 1 route
   Route Flags: R - RIP
            A - Aging, S - Suppressed, G - Garbage-collect
--------------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
      Destination/Mask       Nexthop     Cost  Tag     Flags   Sec
        10.1.1.0/24        192.168.1.2      1    0        RA      32
        172.16.1.0/24       192.168.1.2      1    0        RA      32
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

2)　RIP 与 BFD 联动

双向转发检测 BFD (Bidirectional Forwarding Detection)是一种用于检测邻居路由器之间链路故障的检测机制，它通常与路由协议联动，通过快速感知链路故障并通告使得路由协

议能够快速地重新收敛，从而减少由于拓扑变化导致的流量丢失。

假设有如图 3-6 所示的网络拓扑结构，Router A、Router B 通过二层交换机 switch 互连，在设备上运行 RIP 协议来建立路由，同时使能允许 RIP 在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 RIP 协议，触发协议快速收敛。

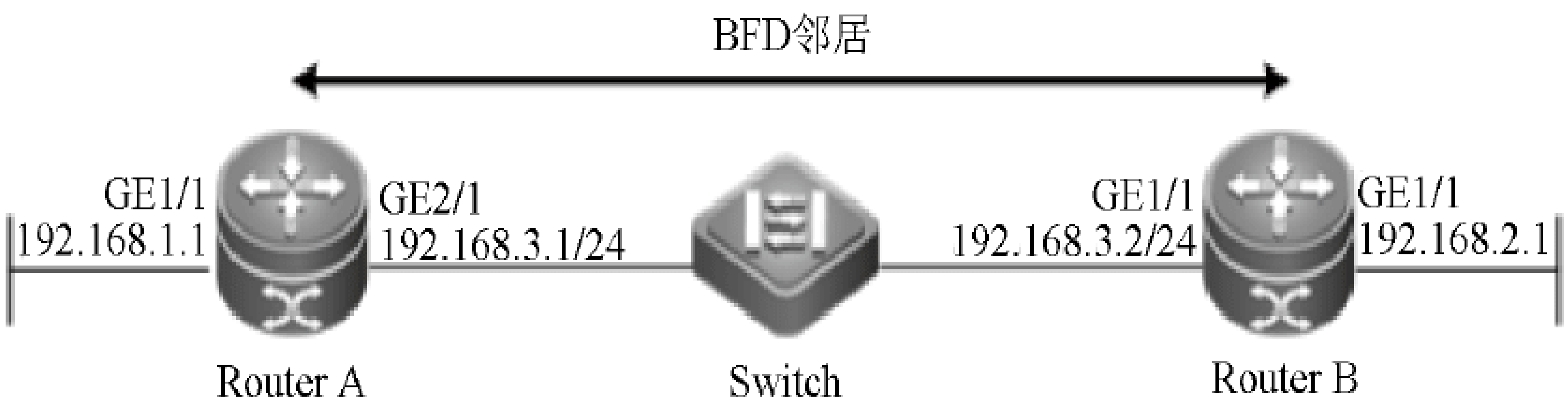


图 3-6 网络拓扑结构

Router A 配置：

(1) 配置 RIP 路由。

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1

RSR-A(config-GigabitEthernet 1/1)#ip ref
RSR-A(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
RSR-A(config-router)# router rip
RSR-A(config-router)# version 2
RSR-A(config-router)# network 192.168.3.0
RSR-A(config-router)# network 192.168.1.0
```

(2) 配置 RIP 与 BFD 联动。

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//配置 BFD 时间参数，该命令同时启用了接口的 BFD 功能，因此必须配置
```

这里的 500/500/3 为推荐配置，间隔 500ms 发送一个探测报文，连续 3 个没收到回应宣告链路失败。

```
RSR-A(config-GigabitEthernet 2/1)#no bfd echo
//推荐配置为该模式(ctrl 模式)，默认是 bfd echo 模式
```

和友商对接更是推荐 ctrl 模式，否则可能对接不起来。

```
RSR-A(config-GigabitEthernet 2/1)#ip rip bfd
//在对应的接口开启 RIP 与 BFD 联动功能
```

Router B 配置：

(1) 配置 RIP 路由。

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
```

```
RSR-B(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
RSR-B(config-router)#  router rip
RSR-B(config-router)#  version 2
RSR-B(config-router)#  network 192.168.3.0
RSR-B(config-router)#  network 192.168.2.0
```

(2)　配置 RIP 与 BFD 联动。

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 2/1)#no bfd echo
RSR-B(config-GigabitEthernet 2/1)#ip rip bfd
```

2. 配置 IS-IS 协议

中间系统到中间系统 IS-IS(Intermediate System to Intermediate System)属于内部网关协议 IGP (Interior Gateway Protocol)，用于自治系统内部。为了支持大规模的路由网络，IS-IS 在自治系统内采用骨干区域与非骨干区域两级的分层结构。一般来说，将 Level-1 路由器部署在非骨干区域，Level-2 路由器和 Level-1-2 路由器部署在骨干区域。每一个非骨干区域都通过 Level-1-2 路由器与骨干区域相连。

IS-IS 是一种链路状态路由协议，每一台路由器都会生成一个 LSP，它包含了该路由器所有启用 IS-IS 协议接口的链路状态信息。通过跟相邻设备建立 IS-IS 邻接关系，互相更新本地设备的 LSDB，可以使得 LSDB 与整个 IS-IS 网络的其他设备的 LSDB 实现同步。然后根据 LSDB 运用 SPF 算法计算出 IS-IS 路由。如果此 IS-IS 路由是到目的地址的最优路由，则此路由会下发到 IP 路由表中，并指导报文的转发。

其相关命令如表 3-2 所示。

表 3-2　IS-IS 的相关命令

命　令	功　能
isis [process-id]	创建 IS-IS 进程并进入 IS-IS 视图
Isis circuit-level[level-1|level-1-2|level-2]	设置接口的 Level 级别，默认情况下，接口的 Level 级别为 Level-1-2
Network-entity net	设置网络实体名称
Net	格式为 x…x.xxxx.xxxx.xxxx.00，前面的“x…x”是区域地址，中间的 12 个“x”是路由器的 System ID，最后的“00”是 SEL
Isis enable[process-id]	指定 IS-IS 的进程号，默认为 1，IS-IS 将通过该接口建立邻居、扩散 LSP 报文
Display isis peer	查看 IS-IS 的邻居信息
Display isis route	查看 IS-IS 的路由信息

3. 配置 OSPF 协议

开放最短路径优先协议是重要的路由选择协议，它是一种链路状态路由选择协议，是由 Internet 工程任务组开发的内部网关路由协议，用于在单一自治系统内决策路由。

链路是路由器接口的另一种说法，因此，OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。下面分别介绍 OSPF 协议的相关要点。

(1) 自治系统。自治系统包括一个单独管理实体下所控制的一组路由器，OSPF 是内部网关路由协议，工作于自治系统内部。

(2) 链路状态。所谓链路状态，是指路由器接口的状态，例如 Up. Down、IP 地址、网络类型、链路开销以及路由器和它邻接路由器间的关系。链路状态信息通过链路状态通告(Link State Advertisement，LSA)扩散到网络上的每台路由器，每台路由器根据 LSA 信息建立一个关于网络的拓扑数据库。

(3) 最短路径优先算法。OSPF 协议使用最短路径优先算法，利用从 LSA 通告得来的信息计算到达每一个目标网络的最短路径，以自身为根生成一棵树，包含了到达每个目的网络的完整路径。

(4) 路由器标识。OSPF 的路由标识是一个 32 位的数字，它在自治系统中被用来唯一地识别路由器。默认使用最高回送地址，若回送地址没有被配置，则使用物理接口上最高的 IP 地址作为路由器标识。

(5) 邻居和邻接。OSPF 在相邻路由器间建立邻接关系，使它们交换路由信息。邻居是指共享同一网络的路由器，并使用 Hello 包来建立和维护邻居路由器间的邻接关系。

(6) 区域。在 OSPF 网络中使用区域(Area)为自治系统分段。OSPF 是一种层次化的路由选择协议，区域 0 是一个 OSPF 网络中必须具有的区域，也称为主干区域，其他所有区域要求通过区域 0 互联到一起。

其相关命令及说明如表 3-3 所示。

表 3-3 OSPF 的相关命令及功能

命　令	功　能
ospf[process-id|router-id router-id|vpn-instance vpn-instance-name]	启动 OSPF 进程，进入 OSPF 视图
area area-id	创建并进入 OSPF 区域视图
network ip-address wildcard-mask	配置区域所包含的网段
display ospf peer	查看 OSPF 邻居信息
display ospf routing	查看 OSPF 路由信息

4. 配置 BGP 协议

边界网关协议 BGP(Border Gateway Protocol)是一种实现自治系统 AS (Autonomous System)之间的路由可达，并选择最佳路由的距离矢量路由协议。它具有以下特点。

(1) 实现自治系统间通信网络的信息可达，BGP 允许一个 AS 向其他 AS 通告其内部网络的可达性信息，或者是通过该 AS 可达的其他网络的路由信息。

(2) 多个 BGP 路由器之间的协调，如果在一个自治系统内部有多个路由器分别使用 BGP 与其他自治系统中对等路由器进行通信，则通过协调使这些路由器保持路由信息的一致性。

(3) BGP 支持基于策略的路径选择，可以为域内和域间的网络可达性配置不同的策略。

(4) BGP 只需要在启动时交换一次完整信息，不需要在所有路由更新报文中传送完整

的路由数据库信息，后续的路由更新报文只通告网络的变化信息，避免网络变化使得信息量大幅增加。

(5)　在 BGP 通告目的网络的可达性信息时，除了处理指定目的网络的下一跳信息之外，通告中还包括了通路向量，即去往该目的网络时需要经过的 AS 的列表，使接受者能够清楚了解去往目的网络的通路信息。

除了以上这些，BGP 允许发送方把路由信息聚集在一起，用一个条目来表示多个相关的目的网络，以节约网络带宽。允许接收方对报文进行鉴别，以验证发送方的身份等多个特点。

BGP 在不同自治系统(AS)之间进行路由转发，分为 EBGP 和 IBGP 两种情况。EBGP 为外部边界网关协议，用于在不同的自治系统间交换路由信息。IBGP 为内部边界网关协议，用于向内部路由器提供更多信息。

其相关命令及说明如表 3-4 所示。

表 3-4　BGP 的相关命令及功能

命　令	功　能
bgp{as—number-plain|as-number-dot}	启动 BGP，指定本地 AS 编号，并进入 BGP 视图
router-id ipv4-address	配置 BGP 的 Router ID
peer{ipv4-address|ipv6-address}as-number{as-number-plain|as-number-dot}	创建 BGP 对等体
ipv4-family {unicast|multicast}	进入 IPv4 地址族视图
import-route direct	管理 IP 所在的网段路由，并引入 RIP 路由表

3.2.2　典型例题分析

例 1　【说明】(2016 年上半年下午试题二)

某学校的网络拓扑结构图如图 3-7 所示。

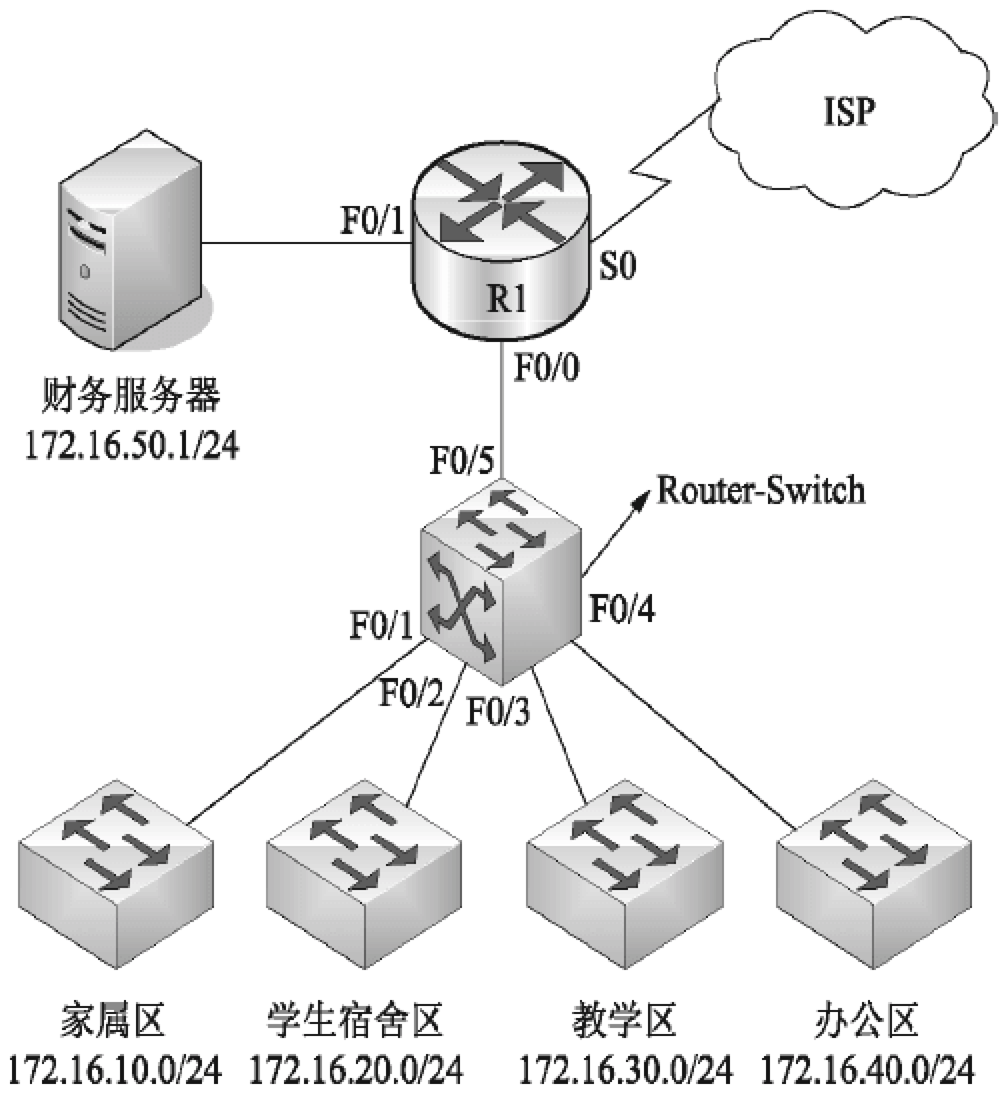


图 3-7　某学校网络拓扑结构图

【问题 1】(每空 1 分，共 7 分)

常用的 IP 访问控制列表有两种，它们是编号为__(1)__和 1300～1399 的标准访问控制列表和编号为__(2)__和 2000～2699 的扩展访问控制列表。其中，标准访问控制列表是根据 IP 报文的__(3)__来对 IP 报文进行过滤，扩展访问控制列表是根据 IP 报文的__(4)__、__(5)__、上层协议和时间等来对 IP 报文进行过滤。一般地，标准访问控制列表放置在靠近__(6)__的位置，扩展访问控制列表放置在靠近__(7)__的位置。

【问题 2】(每空 1 分，共 10 分)

为保障安全，使用 ACL 对网络中的访问进行控制。访问控制的要求如下。

(1) 家属区不能访问财务服务器，但可以访问互联网。

(2) 学生宿舍区不能访问财务服务器，且在每天 18:00—24:00 禁止访问互联网。

(3) 办公区可以访问财务服务器和互联网。

(4) 教学区禁止访问财务服务器，且每天 8:00—18:00 禁止访问互联网。

1. 使用 ACL 对财务服务器进行访问控制，请将下面配置补充完整。

R1(config)#access-list1__(8)__ __(9)__0.0.0.255

R1(config)#access-list1 deny 172.16.10.0 0.0.0.255

R1(config)#access-list1 deny 172.16.20.0 0.0.0.255

R1(config)#access-list1 deny __(10)__0.0.0.255

Rl(config)#interface__(11)__

R1(config-if)#ip access-group1__(12)__

2. 使用 ACL 对 Internet 进行访问控制，请将下面配置补充完整。

```
Route-Switch(config)#time-range jsp //定义教学区时间范围
Route-Switch(config-time-range)# periodic daily (13)
Route-Switch(config)#time-range xsssq //定义学生宿舍区时间范围
Route-Switch(config-time-range)#periodic (14) 18:00 t0 24:00
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 100 permit ip 172.16.10.0 0.0.0.255 any
Route-Switch(config)#access-list 100 permit ip 172.16.40.0 0.0.0.255 any
Route-Switch(config)#access-list 100 deny ip (15) 0.0.0.255 time-range jsp
Route-Switch(config)#access-list 100 deny ip (16) 0.0.0.255 time-range xsssq
Route-Switch (config)#interface (17)
Route-Switch(config-if)# ip access-group 100 out
```

【问题 3】(每空 1 分，共 3 分)

网络在运行过程中发现，家属区网络经常受到学生宿舍区网络的 DDoS 攻击，现对家属区网络和学生宿舍区网络之间的流量进行过滤，要求家属区网络可访问学生宿舍区网络，但学生宿舍区网络禁止访问家属区网络。

采用自反访问列表实现访问控制，请解释配置代码。

```
Route-Switch(config)#ip access-list extended infilter
Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255 reflect
jsp // (18)
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#ip access-list extended outfilter
Route-Switch(config-ext-nacl)# evaluate jsp // (19)
```

```
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#interface fastethernet 0/1
Route-Switch(config-if)#ip access-group infilter in
Route-Switch(config-if)#ip access-group outfilter out // (20)
```

答案：

【问题 1】(每空 1 分，共 7 分)

(1) 1～99　(2) 100～199　(3) 源地址　(4) 源地址　(5) 目的地址

(6) 数据目的地　(7) 数据源

【问题 2】(每空 1 分，共 10 分)

(8) permit　(9) 172. 16. 40. 0　(10) 172. 16. 30. 0　(11) F0/1　(12) out

(13) 8:00 to 18:00　(14) daily　(15) 172. 16. 30. 0　(16) 172. 16. 20. 0　(17) F0/5

【问题 3】(每空 1 分，共 3 分)

(18)当符合任何网络访问 172. 16. 20. 0/16 网络的数据流通过的时候，建立自反控制列表 jsp

(19)计算并生成自反列表

(20)在接口 F0/1 出口方向上应用这个自反列表

解析：

【问题 1】目前常用的 ACL 有两种，分别是标准 ACL 和扩展 ACL，其中，标准 ACL 使用 1～99 以及 1300～1999 的数字作为表号，扩展 ACL 使用 100～199 以及 2000～2699 的数字作为表号。这两种 ACL 的区别是，标准 ACL 只检查数据包的源地址；扩展 ACL 既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。因此，在实际使用中，标准 ACL 的配置位置要尽量靠近目的端，扩展 ACL 的配置位置要尽量靠近源端，这样才能起到最好的效果。

【问题 2】题目要求可以归纳为禁止 IP 地址为 172.16.10.0/24(家属区)、172.16.20.0/24(学生宿舍区)、172.16.30.0/24(教学区)访问 172.16.50.1/24(财务服务器)；允许 IP 地址为 172.16.40.0/24(办公区)访问 172.16.50.1/24; 172.16.10.0/24 和 172.16.40.0/24 可以一直访问互联网；172.16.20.0/2 每天 18:00 到 24:00 禁止访问互联网；172.16.30.0/24 每天 8:00 到 18:00 禁止访问互联网。

禁止某网络地址访问的命令为:access-list [ACL 表号] deny [ip] [mask];

允许某网络地址访问的命令为:access-list [ACL 表号] permit [ip] [mask];

R1(config)#access-list1(permit)(172.616.40.0)　0.0.0.255，permit 语句，允许来自办公区的数据访问；

教学区禁止访问财务服务器用 deny 语句拒绝教学区的 IP 地址；

Rl(config)#interface F0/1 //进去 R1 的 F0/1 端口，不能是 F0/0 接口，以免家属区等不能访问互联网；

R1(config-if)#ip access-group1 out//将 ACL1 设置到 F0/1 端口上，在财务服务器的端口，设置上这个 ACL 表，就可以完成对财务服务器的访问控制了。

要通过 ACL 来限制用户在规定的时间范围内访问特定的服务，首先设备上必须配置好正确的时间范围。时间范围是通过配置 time-range 来实现的。

Route-Switch(config)#access-list 100 deny ip 172.16.30.0 0.0.0.255 time-range jxq //教学区

按 jxq 时间范围禁止访问互联网，教学区 IP 地址为 172.16.30.0;

Route-Switch(config)#access-list 100 deny ip 172.16.40.0 0.0.0.255 time-range xsssq //学生宿舍区按 xsssq 时间范围禁止访问互联网，教学区 IP 地址为 172.16.40.0;

Route-Switch(config)#interface f0/5 //F0/5 端口是交换机连接路由器的端口 Route-Switch (config-if)#ipaccess-group 100 out //将 ACL100 设置到 F0/5 端口上。

【问题 3】根据题意要求在 172.16.10.0/24 的网段上添加对于 172.16.20.0/24 网段的自反访问列表。

自反访问列表 ReflexiveAccessLists，根据一个方向的访问控制列表，自动创建出一个反方向的控制列表，是和原来的控制列表的 IP 的源地址和目的地址颠倒，并且源端口号和目的端口号完全相反的一个列表。并且还有一定的时间限制，过了时间，就会超时，一旦超时，这个新创建的列表就会消失，这个方法能大大增加安全性。

Route-Switch(config)#ip access-list extended infilter //建立名为 infilter 的访问策略，因为这个策略准备设置在流量的入口，取名为 infilter;

Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255reflect jsq //当符合任何网络访问 172.16.20.0/16 网络的数据流通过的时候，建立自反控制列表 jsp;

Route-Switch(config-ext-nacl)#evaluate jsq//计算并生成自反列表;

Route-Switch(config-if)#ip access-group outfilter out//在接口 F0/1 出口方向上应用这个自反列表。

例 2 【说明】(2014 年下半年下午试题三)

某企业的网络结构如图 3-8 所示。

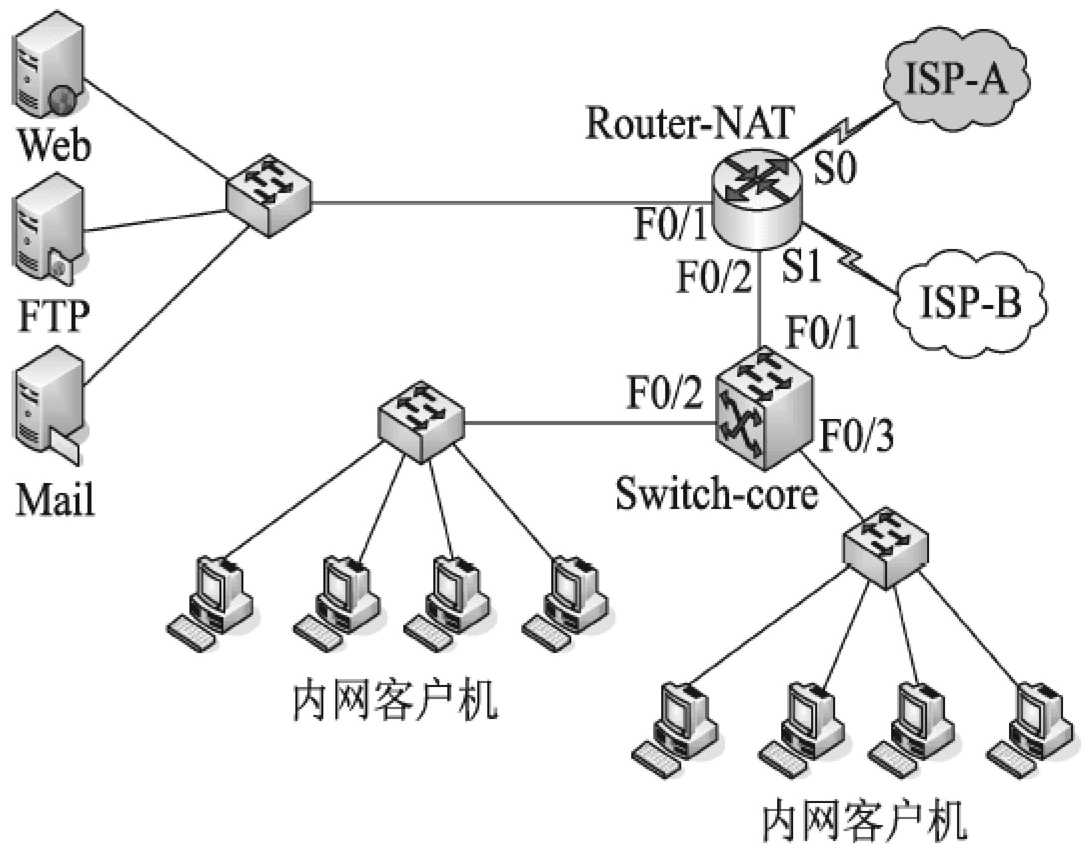


图 3-8 企业网络拓扑结构

按照网络拓扑结构为该企业网络进行网络地址配置，地址分配如表 3-5 所示。

表 3-5 网络地址分配表

设 备	地 址
Router-NAT	F0/1: 192.168.1.1/24 S0: 61.192.93.100/24 S1: 202.102.100.100/24
Web 服务器	192.168.1.100

续表

设　备	地　址
ISP-A	61.192.93.200/24
ISP-B	202.102.100.200/24
ISP-A 地址池	61.192.93.100～61.192.93.102
ISP-B 地址池	202.102.100.100～202.102.100.102

【问题 1】(4 分)

企业网络中使用私有地址，如果内网用户要访问互联网，一般用__(1)__技术将私有网路地址转换为公网地址。在用该技术时，往往是用__(2)__技术指定允许转换的内部主机地址范围。一般来说，企业内服务器需要被外部用户访问，就必须对其做地址变换，内部服务器映射的公共地址不能随意更换，需要使用__(3)__技术。但是对于企业内部用户来讲，使用一一映射的技术为每个员工配置一个地址很不现实，一般使用__(4)__NAT 技术以提高管理效率。

【问题 2】(7 分)

一般企业用户可能存在于任何一家运营商的网络中，为了确保每个运营商网络中的客户都可以高效地访问本企业所提供的网络服务，企业有必要同时接入多个运营商网络，根据企业网络的拓扑图和网络地址规划表，实现该企业出口的双线接入。

首先，为内网用户配置 NAT 转换，其中以 61.192.93.0/24 代表 ISP-A 所有网段；其次为外网用户访问内网服务器配置 NAT 转换。根据需求，完成以下 Route-NAT 的有关配置命令。

Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255

//定义到达 ISP-A 所有网段的 ACL

Route-Switch(config)#access-list 101__(5)__ip any 61.192.93.0 0.0.0.255

Route-Switch(config)#access-list 101__(6)__

//定义到达 ISP-B 所有网段的 ACL

Route-Switch(config)#ip nat pool ISP-A__(7)__netmask 255.255.255.0

//定义访问 ISP-A 的合法地址池

Route-Switch(config)#ip nat pool ISP-B__(8)__netmask 255.255.255.0

//定义访问 ISP-B 的合法地址池

Route-Switch(config)#ip nat inside source list100 pool ISP-A overload

Route-Switch(config)#ip nat inside source__(9)__

//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换

Route-Switch(config)#ip nat inside source static tcp__(10)__extendable

//为内网 Web 服务器配置 ISP-A 的静态 NAT 转换

Route-Switch(config)#ip nat inside source static tcp__(11)__extendable

//为内网 Web 服务器配置 ISP-B 的静态 NAT 转换

【问题 3】(6 分)

在路由器的内部和外部接口启用 NAT，同时为了确保内网可以访问外部网络，在出口

设备配置静态路由，根据需求，完成(或解释)Route-NAT 的部分配置命令。

Route-Switch(config)#int S0

Route-Switch(config)#__(12)__//指定 NAT 的外部转换接口

Route-Switch(config)#int S1

Route-Switch(config)#__(13)__//指定 NAT 的外部转换接口

Route-Switch(config)#int fo/1

Route-Switch(config)#__(14)__//指定 NAT 的内部转换接口

Route-Switch(config)#__(15)__//配置到达 ISP-A 的流量从 S0 口转发

Route-Switch(config)#__(16)__//配置默认路由指定从 S1 口转发

Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 S0 120　　//__(17)__

【问题 4】(3 分)

QoS(服务质量)主要用来解决网络延迟和阻塞等问题，它主要有三种服务模型，分别为__(18)__模型、Integrated service(集成服务)模型及__(19)__模型，其中使用比较普遍的方式是__(20)__模型。

答案：

【问题 1】

(1) NAT　(2) ACL　(3) 静态 NAT　(4) 端口复用

【问题 2】

(5) Deny

(6) permit ip any 202.102.100.0 0.0.0.255

(7) 61.192.93.100 61.192.93.102

(8) 202.102.100.100 202.102.100.102

(9) list 101 pool ISP-B overload

(10) 192.168.1.100 61.192.93.100 80

(11) 192.168.1.100 202.102.100.100 80

【问题 3】

(12) IP NAT OUTSIDE

(13) IP NAT OUTSIDE

(14) IP NAT INSIDE

(15) IP ROUTE 61.192.93.0 255.255.255.0 S0

(16) IP ROUTE 0.0.0.0 0.0.0.0 S1

(17) 配置浮动默认路由

【问题 4】

(18) 区分服务

(19) 尽力而为服务

(20) 尽力而为服务

解析：

【问题 1】本问题主要考查 NAT 转换的相关知识。

一般来说，由于企业内网大都使用私有网络地址，私有地址只能在局域网中使用，不

能出现在互联网上，那么使用私有地址的内部主机想要访问互联网，就必须使用地址转换技术将其转换为公有地址，也就是说如果内网用户想要访问互联网，就必须使用 NAT 地址转换技术，将私有地址转换为在互联网应用的公有地址。在使用 NAT 地址转换技术时，往往要使用 ACL 技术来指定允许转换的内部主机地址范围。

根据映射的方式，可以将 NAT 技术分为静态 NAT 和动态 NAT。其中，静态 NAT 是手工配置的内部私有地址和外部公共地址的对应关系，除非人工修改，否则不会变化，一般对外发布服务器使用静态 NAT 技术。动态 NAT 是多个内部主机和外部公共地址随机对应的一种方式，主要是通过指定内部允许转换的地址范围和外部允许使用的地址范围，然后对两个范围映射。这样具体外部的一个公共地址被内部哪台主机使用不确定。主要适用于企业内网大量用户的客户端访问外网。

【问题 2】一个公司会与两个服务器供应商连接，这样做有利于提高内部访问 Internet 的速度和外网访问内部服务器的速度。由拓扑图可以看出该公司的出口路由器 Router-NAT 将 LAN 和 ISP-A 以及 ISP-B 连接，在 LAN 中有一台 Web 服务器需要发布到 Internet 上供外网访问。Router-NAT 上 S0 的接口地址是 61.192.93.100/24，可用于 NAT 的地址是 61.192.93.100～61.192.93.102，对端 ISP-A 的地址是 61.192.93.200/24。Router-NAT 上 S1 的接口地址是 202.102.100.100/24，可用于 NAT 的地址是 202.101.100.100～202.102.100.102，对端 ISP-B 的地址是 202.102.100.200。Router-NAT 内网口的地址是 192.168.1.1/24。

(1)　定义访问控制列表，由于需要根据访问的 IP 地址的不同来选择进行转换的 NAT 地址，所以需要使用扩展访问控制列表，控制 PAT 转换使用的地址池。

Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255

//定义到达 ISP-A 所有网段的 ACL

Route-Switch(config)#access-list 101(deny)ip any 61.192.93.0 0.0.0.255

Route-Switch(config)#access-list 101(permit ip any 202.102.100.0 0.0.0.255)

//定义到达 ISP-B 所有网段的 ACL

Access-list 100 定义了到达 ISP-A 的所有网段的 ACL，此处 61.192.93.0 代表 ISP-A 所有网段。

(2)　定义合法的地址池。

Route-Switch(config)#ip nat pool ISP-A(61.192.93.101 61 192.93.102)netmask 255.255.255.0

//定义访问 ISP-A 的合法地址池

Route-Switch(config)#ip nat pool ISP-B(202.102.100.101 202.102.100.102)netmask 255.255.255.0

//定义访问 ISP-B 的合法地址池

(3)　配置 PAT 转换。

Route-Switch(config)#ip nat inside source list 100 pool ISP-A overload

Route-Switch(config)#ip nat inside source(list 101 pool ISP-B overload)

//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换

(4)　配置静态 NAT，实现外网访问内网服务器。

Route-Switch(config)#ip nat inside source static tcp (192.168.1.100 61.192.93.100)

extendable

//为内网 Web 服务器配置 ISP-A 的静态 NAT 转换

Route-Switch(config)#ip nat inside source static tcp (192.168.1.100 202.102.100.100) extendable

//为内网 Web 服务器配置 ISP-B 的静态 NAT 转换

【问题 3】通过路由选择原则，将 ISP-A 的目的地址配置静态路由并且下一跳指向 ISP 的路由器，再配置一条默认路由并且其下一跳指向 ISP-B 的路由器，最后再配置一条管理距离为 120 的默认路由，用以备份。

【问题 4】QoS(Quality of Service，服务质量)指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等，但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。通常 QoS 提供以下三种服务模型:

- Best-Effort service(尽力而为服务模型);
- Integrated service(综合服务模型，简称 Int-Serv);
- Differentiated service(区分服务模型，简称 Diff-Serv)。

3.2.3 同步练习

1. 【说明】(2017 年上半年下午试题四)

图 3-9 为某学校网络拓扑图，运营商分配的公网 IP 地址为 113.201.60.1/29，运营商网关地址为 113.201.60.1，内部用户通过路由器代理上网，代理地址为 113.201.60.2。核心交换机配置基于全局的 DHCP 服务，为办公楼和宿舍楼用户提供 DHCP 服务。内部网络划分为 3 个 VLAN，其中 VLAN10 的地址为 10.0.10.1/24，VLAN20 的地址为 10.0.20.1/24，VLAN30 的地址为 10.0.30.1/24，请结合图 3-9，回答相关问题。

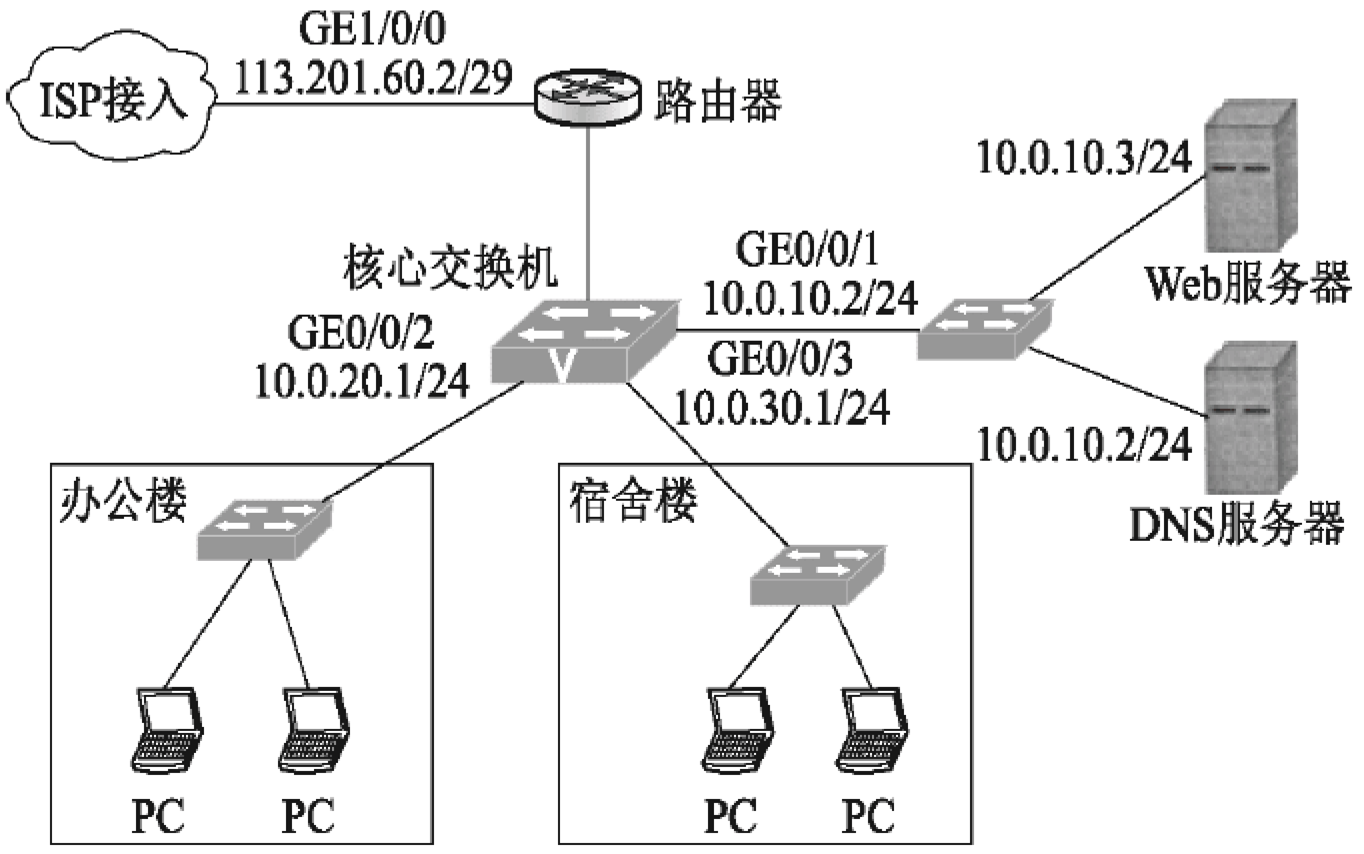


图 3-9　某学校网络拓扑图

【问题 1】(共 9 分)

路由器的配置片段如下，根据图 3-9，补齐(1)～(6)空缺的命令。

```
<Huawei>system-view
[Huawei] sysname (1)
[Router] interface  (2)
[Router-GigabitEthernet1/0/0] ip address (3)
[Router-GigabitEthernet1/0/0] quit
[Router] ip route-static 0.0.0.0 0.0.0 (4)
[Router-acl-basic-2000]
[Router-acl-basic-2000] rule 5 permit source 10.0.0.0 (5)
[Router-acl-basic-2000] quit
[Router] interface GigabitEthernet1/0/0
[Router-GigabitEthernet1/0/0] nat outbound (6)
[Router-GigabitEthernet1/0/0] quit
```

其他配置略。

【问题 2】(共 6 分)

核心交换机的配置片段如下，根据图 3-9，补齐(7)～(10)空缺的命令。

```
#配置 GE0/0/2 接口加入 VLAN20，并配置对应 VLAN 接口地址
[Switch]vlanbatch20
[Switch]inlterface GigabitEthernet0/0/2
[Switch-GigabitEthernet0/0/2]port link-type (7)
[Switch-GigabitEthernet0/0/2]port hybrid pvid vlan20
[Switch-GigabitEthernet0/0/2]port hybrid untagged vlan20
[Switch-GigabitEthernet0/0/2]quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address (8)
[Switch-Vlanif20] quit
```

其他配置略。

```
#配置 DHCP 服务，租期 3 天
[Switch] dhcp (9)
[Switch] ip pool pooll
[Switch-ip-pool-pooll] network 10.0.20.0 mask 225.225.255.0
[Switch-ip-pool-pooll] dns-list 10.0.10.2
[Switch-ip-pool-pooll] gateway-list 10.0.20.1
[Switch-ip-pool-pooll] lesae day (10)
[Switch-ip-pool-pooll] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] dhcp select global
[Switch-Vlanif20] quit
```

其他配置略。

2. 【说明】(2016 年下半年下午试题四)

某公司建立局域网拓扑图如图 3-10 所示。公司计划使用路由器作为 DHCP 服务器，根据需求，公司内部使用 C 类地址段，服务器地址段为 192.168.2.0/24，S2 和 S3 分别为公司两个部门的接入交换机。分别配置 VLAN 10 和 VLAN 20，地址段分别使用 192.168.10.0/24

和 192.168.20.0/24，通过 DHCP 服务器自动为两个部门分配 IP 地址，地址租约期为 12 小时。其中，192.168.10.1～192.168.10.10 作为保留地址。

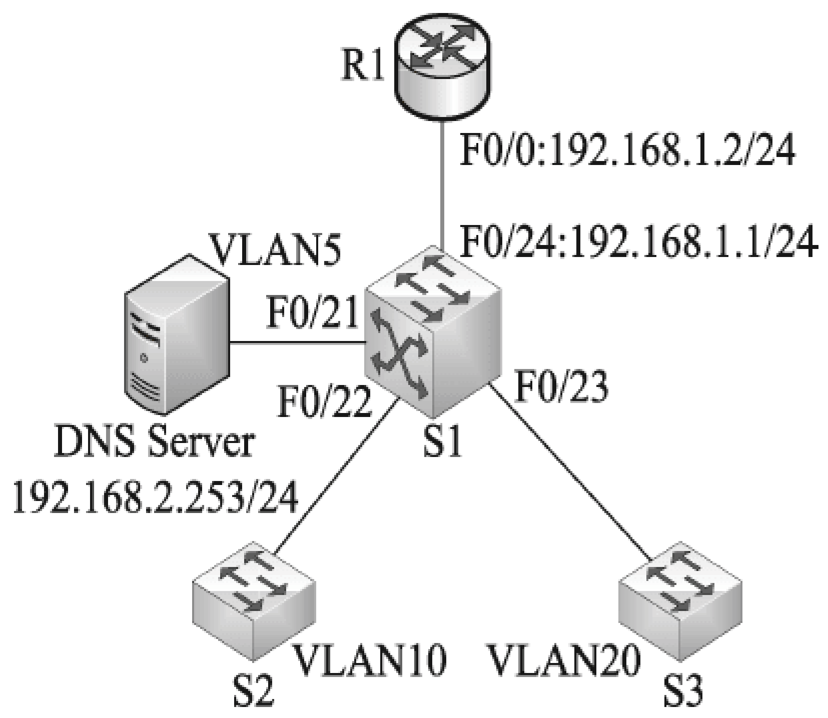


图 3-10　局域网拓扑图

【问题 1】(10 分，每空 1 分)

下面是 R1 的配置代码，请将下面配置代码补充完整。

```
R1#config t
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address___(1)___ ___(2)___
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp___(3)___depart1
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.254 255.255.255.0
R1(dhcp-config)#dns-server___(4)___
R1(dhcp-config)#lease 0 ___(5)___ 0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool depart2
R1(dhcp-config)#network___(6)___ ___(7)___
R1(dhcp-config)#default-router 192.168.20.254 255.255.255.0
R1(dhcp-config)#dns-server 192.168.2.253
R1(dhcp-config)#lease 0 12 0
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address
R1(config)#ip dhcp excluded-address___(8)___ ___(9)___
R1(config)#ip dhcp excluded-address___(10)___//排除掉不能分配的 IP 地址
R1(config)#ip dhcp excluded-address 192.168.20.254
```

【问题 2】(5 分，每空 1 分)

下面是 S1 的配置代码，请将下面配置代码或解释补充完整。

```
S1#config terminal
S1(config)#interface vlan 5
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan 10
S1(config-if)#ip helper-address___(11)___    //指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan 20
…
```

```
S1(config)#interface f0/24
S1(config-if)#switchport mode__(12)__
S1(config-if)#switchport trunk__(13)__vlan all  //允许所有 VLAN 数据通过
S1(config-if)#exit
S1(config)#interface f0/21
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 5
S1(config-if)#exit
S1(config)#interface f0/22
S1(config-if)#switchport mode access
S1(config-if)#switchport access__(14)__
S1(config)#interface f0/23
S1(config-if)#switchport mode access
S1(config-if)#switchport access__(15)__
```

3.2.4　同步练习参考答案

1. 答案：

【问题 1】

(1) Router　(2) GigabitEthernet 1/0/0　(3) 113.201.60.2　255.255.255.248

(4) 113.201.60.1　(5) 0.0.255.255　(6) 2000

【问题 2】

(7) hybrid　(8) 10.10.20.1 255.255.255.0　(9) enable　(10) 3

解析：

【问题 1】

(1) 重命名设备　(2) 进入端口子模式　(3) 给端口配置 IP 和掩码

(4) 配置默认路由，下一跳指向 ISP 地址　(5) 配置反掩码

(6) 把符合 ACL2000 的地址做 NAT 转换

【问题 2】

(7) 除了 Access 类型和 Trunk 类型外，交换机还支持第三种 Hybird 类型端口。这种接口可以接收和发送多个 VLAN 数据帧，同时还能指定对任何 VLAN 帧进行剥离标签操作。

(8) 配置接口 IP 和掩码

(9) dhcp enable：开启 dhcp 配置

(10) lease day 3：配置租约期为 3 天

2. 答案：

【问题 1】

(1) 192.168.1.2　(2) 2 55.255.255.0　(3) pool　(4) 192.168.2.253

(5) 12　(6) 192.168.20.0　(7) 255.255.255.0　(8) 192.168.10.1

(9) 192.168.10.10　(10) 192.168.10.254

【问题 2】

(11) 192.168.1.2　(12) trunk　(13) allowed　(14) vlan 10　(15) vlan 20

解析：

【问题 1】

根据网络拓扑图可知 F0/0 的 IP 地址为 192.168.1.2，子网掩码为 255.255.255.0。空(3)表示设置 dhcp 地址池，空(4)为设置 DNS 服务器地址，即 192.168.2.253，空(5)R1(dhcp-config)#lease 0 12 0 表示设定 DHCP 地址租约为 12 小时，空(6)、(7)表示部门 2 使用 192.168.20.0/24，设置 VLAN20 的网络地址 R1(dhcp-config)#network 192.168.20.0 255.255.255.0，其中 192.168.10.1～192.168.10.10 地址保留不分配，所以：

R1(config)# ipdhcp excluded-address 192.168.10.1 192.168.10.10

R1(config)# ipdhcp excluded-address 192.168.10.254 //排除掉不能分配的 IP 地址

【问题 2】

S1(config-if)# ip helper-address 192.168.1.2 //指定 DHCP 服务器的地址

该企业使用路由器作为 DHCP 服务器，故所填地址即为路由器的地址。trunk 模式的端口用于交换机与交换机，交换机与路由器，大多用于级联网络设备。access 多用于接入层，也叫接入模式，主要是将端口静态接入。默认情况下 trunk 允许所有的 VLAN 通过，即 S1(config-if)# switchport trunk allowed vlan all //允许所有 VLAN 数据通过。由题意知，部门 1 使用的是 VLAN 10，interface f0/22，部门 2 使用的是 VLAN 20，interface f0/23，所以空(14)填写 vlan 10，空(15)填写 vlan 20。

3.3 网络接入方式

3.3.1 考点辅导

3.3.1.1 接入网的定义

计算机通信网包含传输骨干网、城域交换网和社区接入网三部分。传输骨干网是连接各个城域网信息的高速公路，是网络技术的关键，它提供远距离、高带宽、大容量的数据传输业务；城域交换网将各个单位、社区的局域网相连接，实现数据的高速传输和信息资源共享；社区接入网解决的是从市区到小区，直至到每个家庭用户的终端接入问题，即最后一千米(Last Kilometer)的问题。

所谓接入网是指从交换机到用户终端之间的所有接线设备，如图 3-11 所示。

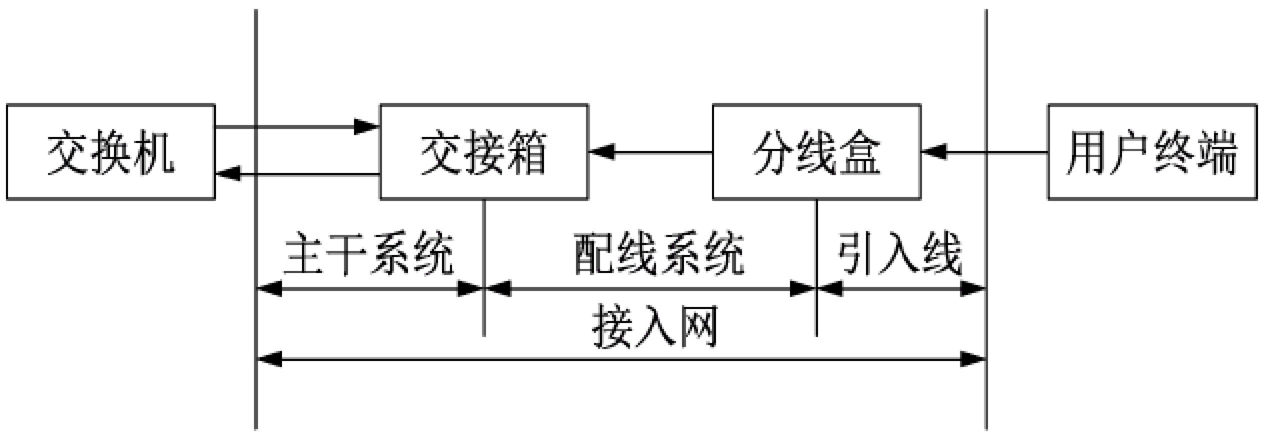


图 3-11 接入网的位置

其中，主干系统为传统的电缆和光缆，一般长数千米；配线系统也可能是电缆和光缆，其长度一般为几百米；而引入线通常长几米到几十米。国际电信联盟远程通信标准化组

(ITU-T)根据近年来电信网的发展演变趋势，提出了接入网的概念，其目的是综合考虑本地交换机、用户环路和终端设备，通过有限的标准接口，将各种用户接入到业务节点。ITU-T 规定，接入网是指由业务节点接口(SN)和相关用户网络接口(UNI)之间的一系列传送实体所组成，是为传送电信业务提供其所需传送承载能力的实施系统，它可以经由电信网标准 Q3 接口进行配置和管理。

接入网所包括的范围可由 3 个接口来标志。在网络侧它通过节点接口与业务节点相连；在用户侧经由用户网络接口与用户终端相连；而管理功能则通过 Q3 接口与电信管理网(TMN)相连来实现。

其中业务节点接口(Service Node Interface，SNI)是提供业务的实体。它是一种可以接入各种交换型、半永久连接型电信业务的网元。SNI 可提供规定业务的业务节点，有本地交换机、租用线业务节点或特定配置下的点播电视和广播电视业务节点等。SNI 是 AN 与 SN 之间的接口。

3.3.1.2　接入网的主要功能和特点

接入网是业务提供点与最终用户之间的连接网络，其主要功能如下。

- 用户口功能(UPF)：将特定的 UNI 规定的要求与核心功能和管理功能相适配。
- 业务口功能(SPF)：将特定的 SNI 规定的要求与公用承载通路相适配。
- 核心功能(CF)：处于 UPF 和 SPF 之间，主要作用是负责将个别用户口承载通路或业务口承载通路规定的要求与公用传送承载通路相适配。其功能还包括提供通过 AN 传送所需要的协议适配和处理复用所进行的协议承载通路。
- 传送功能(TF)：为 AN 中不同地点之间公用承载通路的传送提供通道，也为传输媒质提供媒质适配功能。
- AN 系统管理功能(SMF)：协调 AN 内 UPF、SPF、CF 和 TF 的适配、维护和操作，也负责协调用户终端和业务节点的操作功能。

作为业务提供点与最终用户之间的接口网络，接入网具有以下特点。

- 主要完成复用、交叉连接和传输功能，不具备交换功能。
- 提供开放的 V5 标准接口，可实现与任何种类的交换设备进行连接。
- 光纤化程度高。
- 能提供各种综合业务。
- 对环境的适应能力强。
- 组网能力强。
- 可采用 HDSL、ADSL、有源或无源光网络、HFC 和无线网等多种接入技术。
- 接入网可独立于交换机进行升级，灵活性高，有利于引入新业务和向宽带网过渡。
- 接入网提供了功能较为全面的网管系统，实现了对接入网内所有设备的集中维护以及环境监控、112 测试等，并可通过相应的协议接入本地网网管中心，给网管带来方便。

3.3.1.3　接入网的分类

通常可以将接入网分为以下几大类。

1. 基于普通电话线的 xDSL 接入

xDSL 可分为 IDSL、HDSL、SDSL、VDSL 和 ADSL，它们均采用点到点的拓扑结构。

2. 同轴电缆上的 HFC/SDV 接入系统

HFC/SDV 都是基于混合光纤同轴电缆上的接入系统，HFC 是双向接入传输系统，SDV 是可交换的数字视频接入系统，它在同轴电缆上只传下行信号。HFC/SDV 的拓扑结构可以是树型或总线型，下行方向通常为广播方式。HFC/SDV 在下行方向上可以混合传送模拟和数字信号。

3. 光纤接入系统

光纤接入系统可分为有源系统和无源系统。有源系统有基于准同步数字系列的，也有基于同步数字系列的，它的拓扑结构可以是环型、总线型、星型或它们的混合型，也有点到点的应用。无源系统有窄带和宽带之分。

4. 无线接入系统

无线接入的主要工作方式是一点到多点，上行解决多用户争用的技术有 FDMA、TDMA、CDMA，从频谱效率来看 CDMA 最好，TDMA 次之。

3.3.1.4 接入网的主要业务

对于小企事业用户和居民用户，近期的主要宽带业务需求主要有下面 5 类。

- 点播电视 VOD(Video On Demand)或 NVOD(Near Video On Demand)，又称影视点播业务或准影视点播业务，尤其是点播电影节目。
- 交互式图像游戏。
- 交互式图像业务。
- 远程教育。
- 多媒体库。

3.3.2 典型例题分析

【说明】某省运营商的社区宽带接入网络结构如图 3-12 所示。

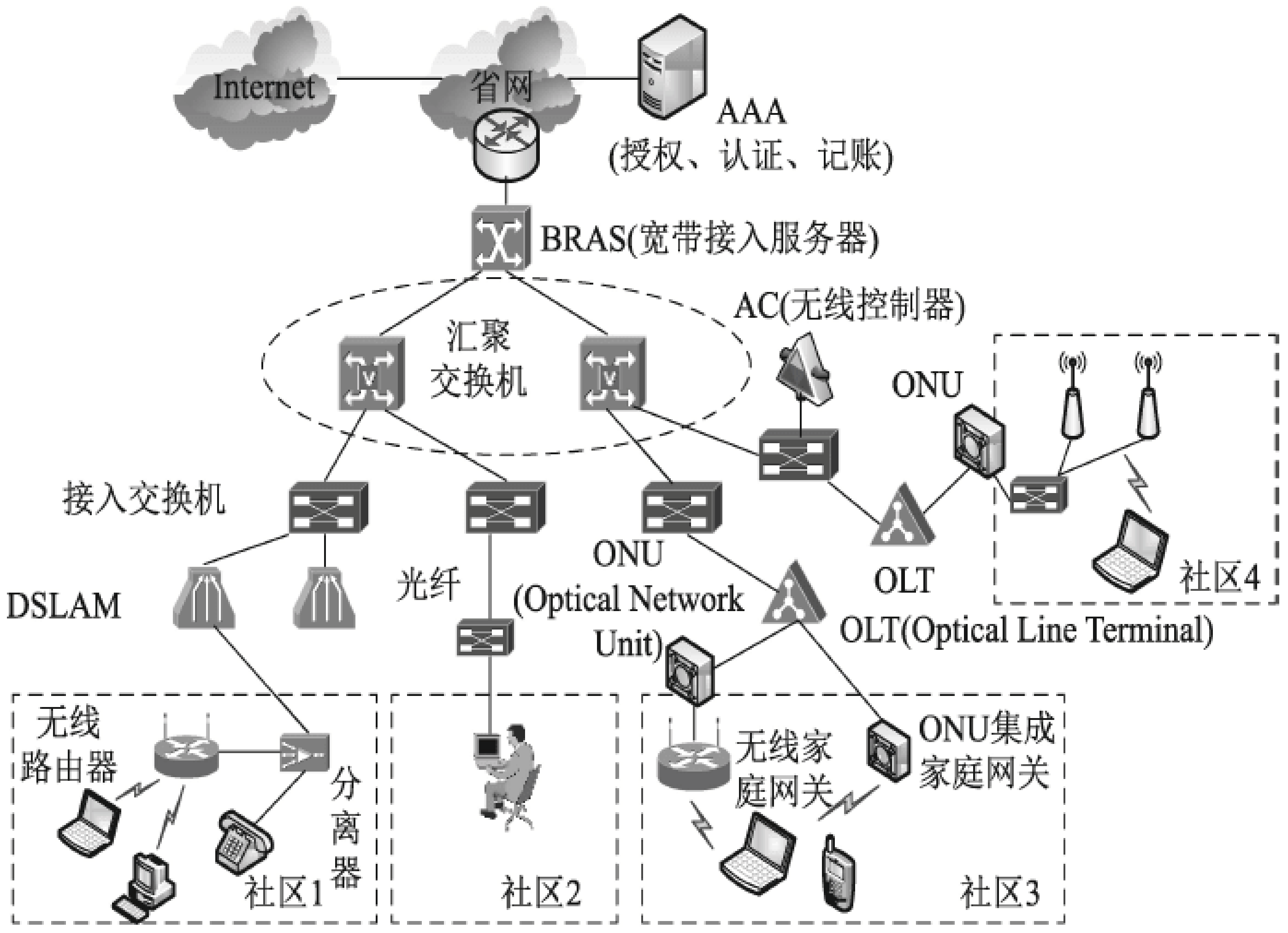


图 3-12 某省运营商的社区宽带接入网络结构图

【问题 1】(7 分)

高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。图 3-11 所示的四个社区采用的小区宽带接入方法分别是：社区 1__(1)__，社区 2__(2)__，社区 3__(3)__，社区 4__(4)__。除了这几种宽带接入方法以外，采用有线电视网进行宽带接入的方法是__(5)__，利用电力网进行宽带接入的方法是__(6)__，IEEE 802.16 标准进行宽带接入的方法是__(7)__。

空(1)～(7)备选答案：

A. FTTx+PON　　B. HFC　　C. FTTx+LAN　　D. WLAN

E. WiMAX　　F. xDSL　　G. PLC(Power-Line Communication)　　H. GPRS

【问题 2】(3 分)

在宽带接入中，FTTx 是速度最快的一种有线接入方式，而 PON(Passive Optical Network)技术是未来 FTTx 的主要解决方案。PON 目前有两种主要的技术分支，分别是 GPON 和 EPON，EPON 是__(8)__技术和__(9)__技术的结合，它可以实现上下行__(10)__的速率。

【问题 3】(6 分)

宽带接入通常采用 PPPoE 进行认证。PPP 协议一般包括三个协商阶段，__(11)__协议用于建立和测试数据链路；__(12)__协议用于协商网络层参数；__(13)__协议用于通信双方确认对方的身份。

【问题 4】(4 分)

在运营商网络中，一般会有多个用户和不同的流需要融合。运营商常用外层 VLAN 区分不同的__(14)__，在 ONU 或家庭网关处采用内层 VLAN 来区分不同的__(15)__；这种处理方式要求运营商网络和用户局域网中的交换机都支持__(16)__协议，同时通过 802.1ad(运营商网桥协议)来实现灵活的 QinQ 技术。

答案：

【问题 1】(1) F　(2) C　(3) A　(4) D　(5) B　(6) G　(7) E

【问题 2】(8) 以太网　(9) PON(或无源光网络)　(10) 1.25Gbps

【问题 3】(11) LCP　(12) NCP　(13) 认证(CHAP/PAP)

【问题 4】(14) 业务　(15) 用户　(16) 802.1q

解析：

【问题 1】高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。图 3-11 所示的四个社区采用的小区宽带接入方法分别是：社区 1 有分离器，采用的是 xDSL。FTTx+LAN 技术是一种利用光纤加超五类网络线方式实现宽带接入方案，实现千兆光纤到小区(大楼)中心交换机，中心交换机和楼道交换机以百兆光纤或五类网络线相连，楼道内采用综合布线，用户上网速率可达 10Mbps，网络可扩展性强，投资规模小。社区 2 是光纤接入，是 FTTx+LAN。社区 3 FTTx+PON，PON 是指光分配网(ODN)不含有任何电子器件及电子电源的网络，其 ODN 全部由光分路器和光缆等无源器件组成。社区 4 采用 WLAN。除了这几种宽带接入方法以外，采用有线电视网进行宽带接入的方法是 HFC，利用电力网进行宽带接入的方法是 PLC(Power-Line Communication)，IEEE 802.16 标准进行

宽带接入的方法是 WiMAX。全球互通微波存取(Worldwide Interoperability for Microwave Access，WiMAX)是一项高速无线数据网络标准，主要用在蜂窝网络，由 WiMAX 论坛提出并于 2001 年 6 月成形。它可提供最后一英里无线宽带接入，作为电缆和 DSL 之外的选择。在 IEEE 802.16 标准的多个版本和选项中做出唯一的选择。

【问题 2】 EPON 即 Ethernet Passive Optical Network，以太网无源光网络。IEEE 802.3 定义了以太网的两种基本操作模式。第一种模式采用载波侦听多址访问/冲突检测(CSMA/CD)协议而应用在共享媒质上；第二种模式为各个站点采用全双工的点到点的链路通过交换机连接到一起。EPON 目前可以提供上下行对称的 1.25Gb/s 的带宽，并且随着以太技术的发展可以升级到 10Gb/s。

【问题 3】宽带接入通常采用 PPPoE 进行认证。PPP 协议一般包括三个协商阶段，LCP 协议用于建立和测试数据链路；NCP 协议用于协商网络层参数；CHAP 协议用于通信双方确认对方的身份。

【问题 4】在运营商网络中，一般会有多个用户和不同的流需要融合。运营商常用外层 VLAN 区分不同的用户，在 ONU 或家庭网关处采用内层 VLAN 来区分不同的业务流。这种处理方式要求运营商网络和用户局域网中的交换机都支持 802.1q 协议，同时通过 802.1ad(运营商网桥协议)来实现灵活的 QinQ 技术。

3.3.3 同步练习

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】 某小区采用 HFC 接入 Internet 的解决方案进行网络设计，网络结构如图 3-13 所示。

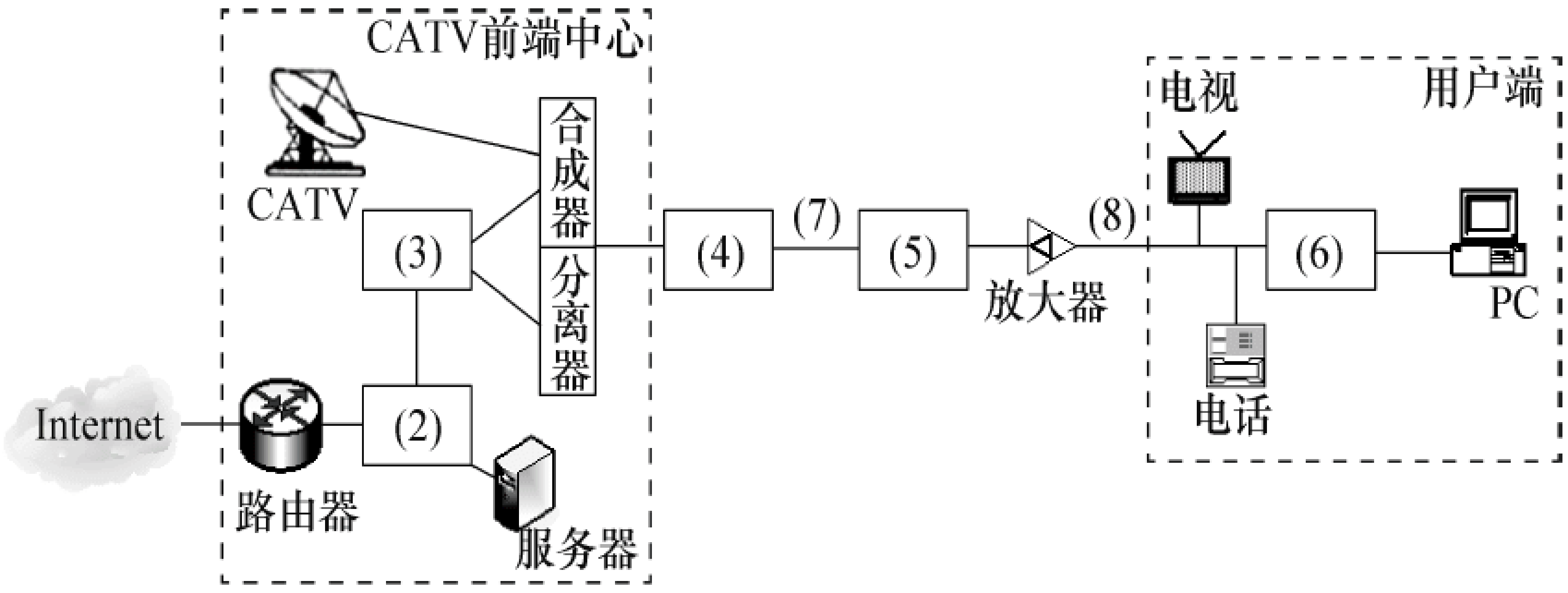


图 3-13 网络结构图

【问题 1】(3 分)

网络设计流程通常由以下 5 个阶段组成。

A. 确定网络物理结构

B. 确定网络逻辑结构

C. 对现有网络的体系结构进行分析

D. 安装和维护

E. 需求分析

根据网络开发设计的过程，给出上述 5 个阶段的先后排序： (1) 。

【问题 2】(5 分)

为图 3-13 中(2)～(6)处选择对应的设备名称，填入答题纸对应的解答栏内。

备选设备：CMTS、以太网交换机、光收发器、光电转换节点、Cable Modem。

【问题 3】(2 分)

在答题纸对应的解答栏内填写图 3-13 中(7)、(8)处对应的传输介质。

【问题 4】(3 分)

Cable Modem 接收从 CMTS 发送来的_(9)_调制信号，经解调后重建以太帧。在相反方向上，接收到的以太帧被封装在时隙中，经_(10)_调制后，通过 HFC 网络的上行信道传送给 CMTS。

(9)、(10)备选答案：

A. QAM　　B. QPSK　　C. GMSK　　D. DMT

【问题 5】(2 分)

有线电视 HFC 网络的上、下行信道是非对称的，容易产生噪声、影响传输质量的是上行信道还是下行信道？

3.3.4　同步练习参考答案

答案：

【问题 1】

(1)　E→C→B→A→D

【问题 2】

(2)　以太网交换机　　(3)　CMTS　　(4)　光收发器

(5)　光电转换节点　　(6)　Cable Modem

【问题 3】

(7)　光缆　　(8)　同轴电缆

【问题 4】

(9)　A　　(10) B

【问题 5】

上行信道

3.4　本 章 小 结

本章知识点在 2014 年的新大纲中变化较小，只是一些表述方式的调整。

本章主要要求考生掌握 IP 地址的规划、路由器的基本配置以及路由协议的相关配置，还有常见的网络接入技术。

本章内容为下午科目的重点内容，尤其是路由器的配置，基本为每次考试的必考内容，而且所占比重很大。

第 4 章　Windows 应用服务器的配置

大纲要求：

- IP 地址，包括 IPv4、IPv6、动态分配和静态分配、DHCP 服务器的原理和配置(Windows)。
- 网络系统管理，包括网络管理命令、Windows 系统、Windows 活动目录、Windows 终端服务与远程管理。
- DNS，包括 URL、域名解析、DNS 服务器的配置(Windows)。
- 电子邮件服务器配置(Windows)。
- WWW，包括虚拟主机、WWW 服务器配置(Windows)、WWW 服务器的安全配置。
- 代理服务器的配置(Windows)。
- FTP 服务器，包括 FTP 服务器的访问、FTP 服务器的配置(Windows)。

4.1　IIS 服务器的配置

4.1.1　考点辅导

4.1.1.1　安装 IIS 7.5

IIS 中集成了多种服务，除了可提供 Web 服务外，还提供用于文件传输的 FTP(文件传输协议)服务、用于邮件服务的 SMTP(简单邮件传输协议)服务和用于新闻组的 NNTP(网络新闻传输协议)服务。Windows Server 2008 R2 中集成了最新的 IIS 7.5，IIS 7.5 包含了 Web 服务器和 FTP 服务器。

下面介绍 IIS 7.5 的安装方法。

(1) 选择“开始”→“管理工具”→“服务器管理器”命令。打开“服务器管理器”窗口后，选择左侧的“角色”节点，在右窗格的“角色摘要”部分中单击“添加角色”超链接，启动添加角色向导。

(2) 在“开始之前”向导页中提示此向导可以完成的工作，以及操作之前应注意的相关事项，然后单击“下一步”按钮。

(3) 在“选择服务器角色”向导页中显示所有可以安装的服务器角色，如果角色前面的复选框没有选中，表示该网络服务尚未安装，如果已选中，说明该服务已经安装。 这里选中“Web 服务器(IIS)”复选框，如图 4-1 所示。

(4) 系统提示在安装 Web 服务器(IIS)角色时，必须要安装 Windows 进程激活服务功能，否则无法安装 Web 服务器(IIS)角色，单击“添加必需的功能”按钮，如图 4-2 所示。

图 4-1　选择服务器角色

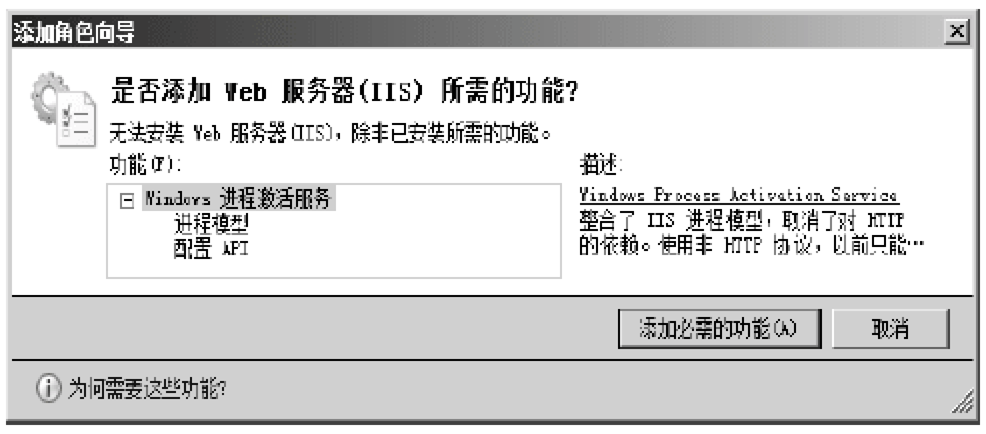


图 4-2　系统提示

(5)　返回“选择服务器角色”向导页后，“Web 服务器(IIS)”复选框被勾选，单击“下一步”按钮。

(6)　在“Web 服务器(IIS)简介”向导页中显示 Web 服务器的功能，注意事项和其他信息，单击“下一步”按钮。

(7)　在“选择角色服务”向导页中默认只选择安装 Web 服务所必需的组件，用户可根据实际需要选择安装的组件。例如，Web 服务器需要使用 APS.NET 或 ASP，则需要选中相应的复选框。选择完毕后，单击“下一步”按钮，如图 4-3 所示。

(8)　在“确认安装选择”向导页中显示前面所进行的设置，如果选择错误，用户可以单击“上一步”按钮返回。确认无误后，用户可以单击“安装”按钮开始安装 Web 服务器角色，如图 4-4 所示。

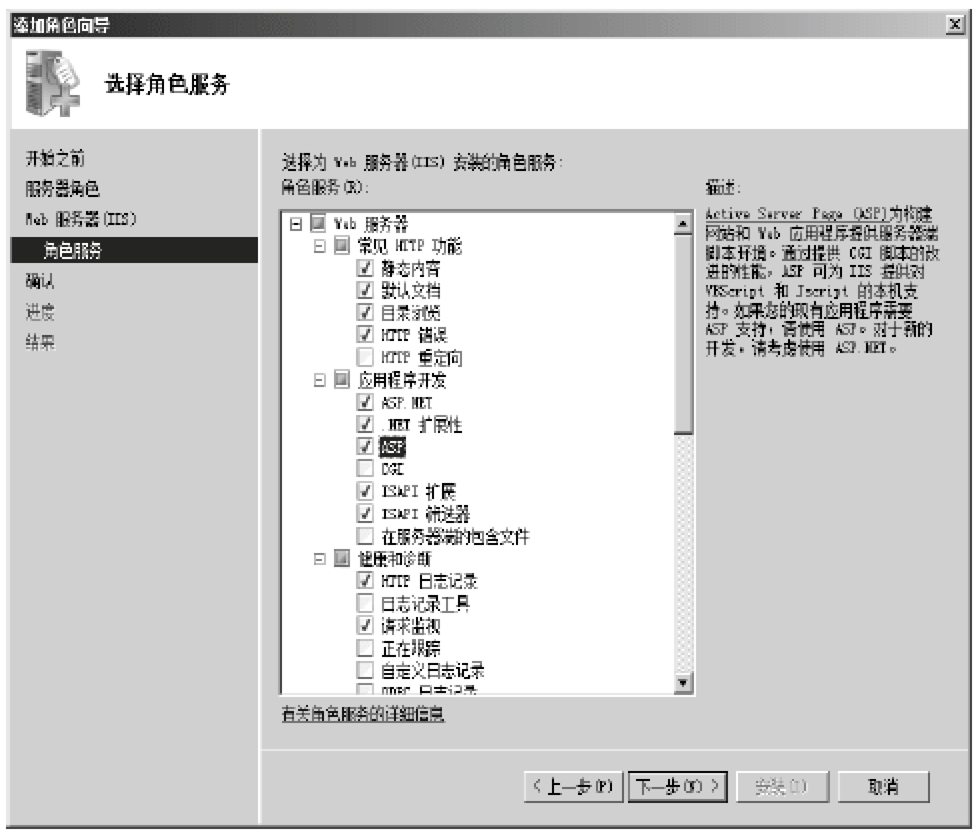


图 4-3　选择角色服务

图 4-4　确认安装选择

(9)　在“安装进度”向导页中显示服务器角色的安装过程。

(10) 在“安装结果”向导页中显示 Web 服务器(IIS)角色已经安装，并列出了已安装的角色服务。单击“完成”按钮，关闭“添加角色向导”向导页，即可完成 Web 服务器(IIS)角色的安装。

(11) 基于 IIS 的 Web 服务器安装成功后，用户可以通过“Internet 信息服务(IIS)管理器”窗口来管理 Web 站点。打开“Internet 信息服务(IIS)管理器”窗口的方法是选择“开始”→“管理工具”→“Internet 服务管理器”命令。图 4-5 所示的是“Internet 信息服务(IIS)管理

器”窗口，从图中可以看出，在安装 IIS 时已创建一个名为 Default Web Site 的 Web 网站。

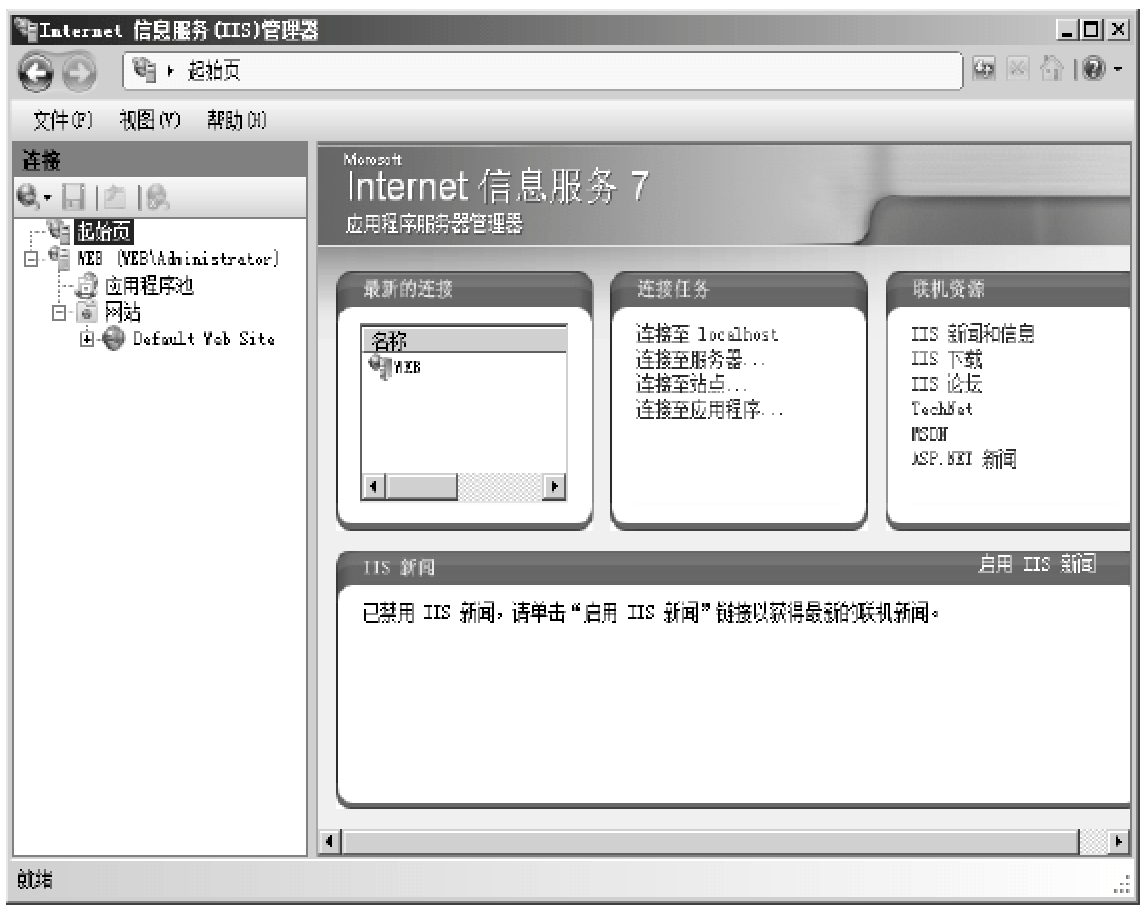


图 4-5　“Internet 信息服务(IIS)管理器”窗口

(12) 在局域网中的另一台计算机上打开浏览器，在地址栏中输入“http://<服务器 IP 或域名>/”，若能看到如图 4-6 所示的界面，则说明 Web 服务器安装成功。

图 4-6　访问 Default Web Site

4.1.1.2　配置 Web 服务器

IIS 7.5 的 Web 服务组件安装成功后，就可以在这台服务器上创建 Web 站点了。默认情况下，在安装的过程中，系统会自动创建一个默认的 Web 站点。用户可以通过修改默认站点的属性发布自己的 Web 网站，也可以重新建立一个 Web 站点。

1. 网站的基本配置

通过“开始”→“管理工具”→“Internet 服务管理器”命令，打开“Internet 信息服务(IIS)管理器”窗口。在管理器的左侧窗格中单击“网站”节点前的“+”号，然后选中某个希望配置的网站，右键单击该网站，在弹出的快捷菜单中选择“属性”命令，打开网站属性对话框。

在“网站”选项卡中可以设置网站的标识，包括网站描述、IP 地址和端口号，还可以设置连接超时、启用日志记录等，从网站日志记录中可以查看哪些用户访问了网站中的哪

些内容，如图 4-7 所示。

在“主目录”选项卡中指定网站 Web 内容的来源，如图 4-8 所示。

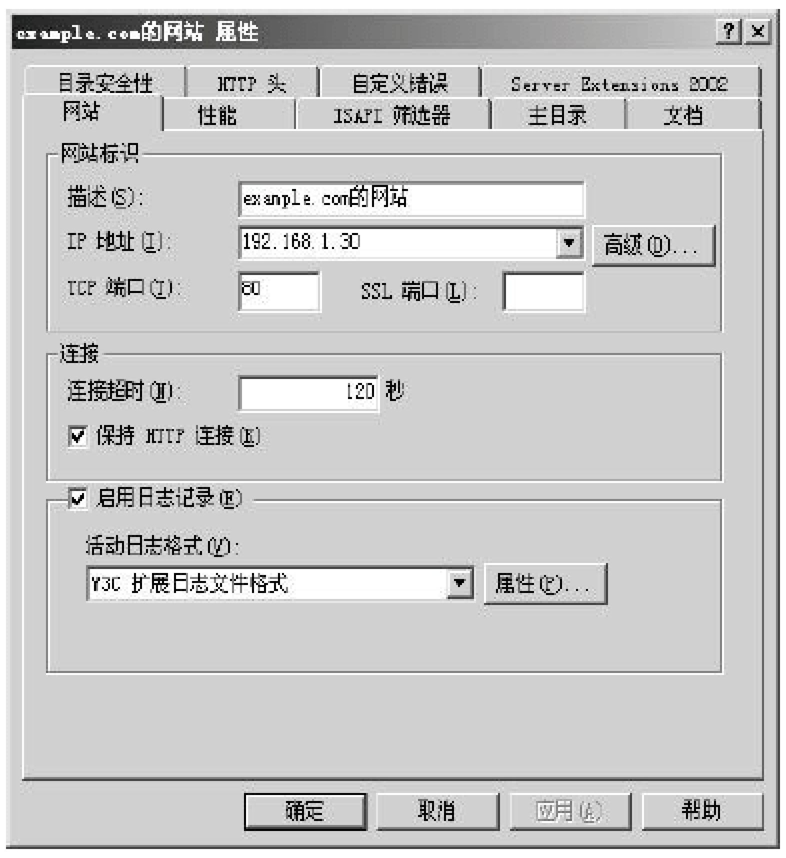


图 4-7　“网站”选项卡

图 4-8　“主目录”选项卡

2. 网站的安全性配置

为了保证 Web 网站和服务器的安全，可以在“目录安全性”选项卡上为网站进行身份验证和访问控制、IP 地址和域名限制的设置，如图 4-9 所示。在“身份验证和访问控制”选项组中单击“编辑”按钮，打开如图 4-10 所示的“身份验证方法”对话框。使用该对话框可以配置 Web 服务器以验证用户身份。可以验证单个用户或选择用户组来阻止未授权用户与受限制内容建立 Web(HTTP)连接。

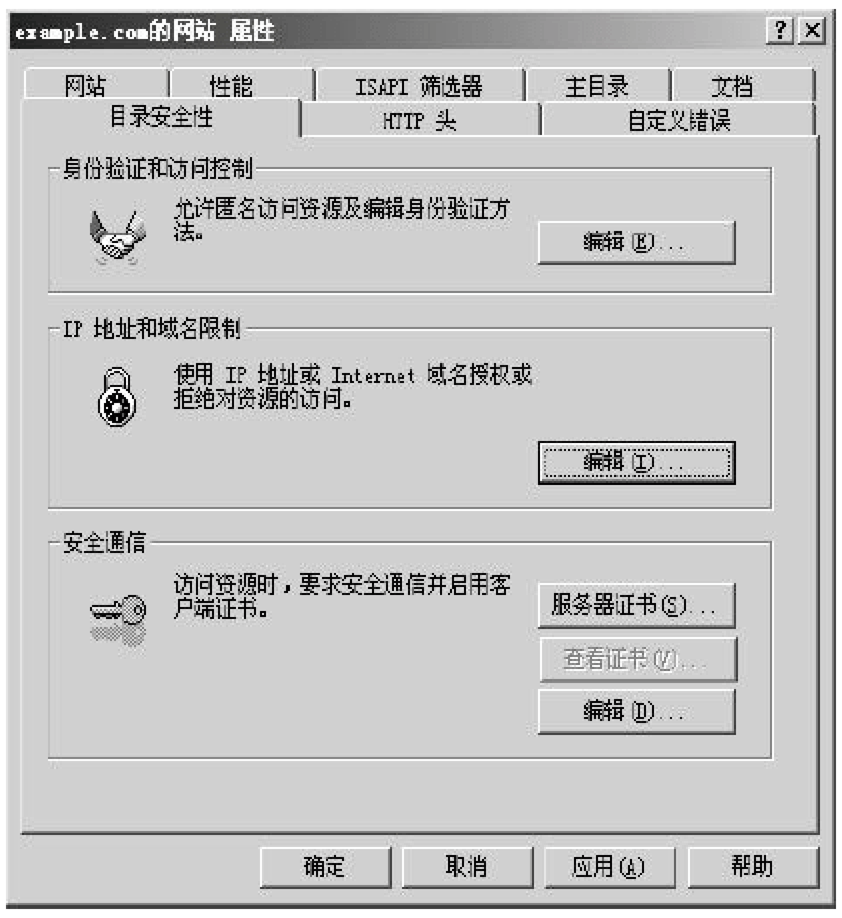


图 4-9　“目录安全性”选项卡

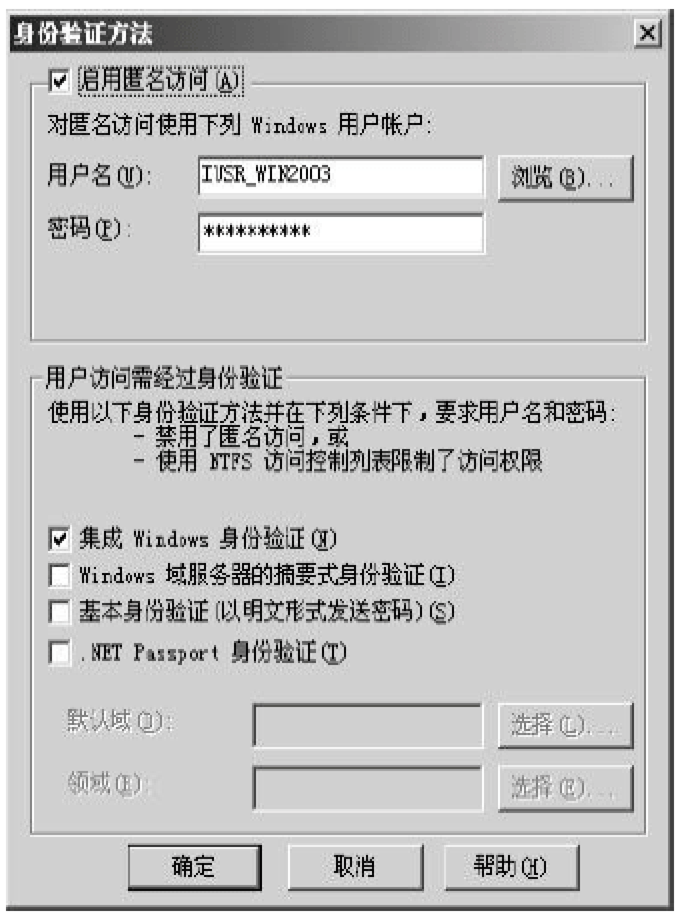


图 4-10　“身份验证方法”对话框

选中“启用匿名访问”复选框可以为用户建立匿名连接，此时用户无须专用的账户，而是使用匿名或来宾账户(Guest)登录到 IIS。默认情况下，服务器创建和使用账户 IUSR_计算机名，对应于本书所举的例子，用户名为 IUSR_WIN2008_R2。

如果用户希望对网站的访问者验证身份，也可以在“身份验证方法”对话框中的“用户访问需经过身份验证”选项组中进行设置。在此部分中选中的选项要求用户在访问服务器上的任何信息前，提供有效的 Microsoft Windows 用户名和密码。当前 IIS 7.5 中提供了以下 3 种身份验证方法。

① 基本身份验证。用户使用基本身份验证访问 Web 站点时，系统会模仿为一个本地用户(即能实际登录到Web服务器的用户)登录到Web服务器，因此用于基本验证的Windows用户必须具有“本地登录”用户权限。它是一种工业标准的验证方法，大多数浏览器支持这种验证方法。在使用基本身份验证方法时，用户密码是以未加密形式在网络上传输的，很容易被蓄意破坏系统安全的人在身份验证过程中使用协议分析程序破译用户和密码，因此这种验证方式是不安全的。

② 摘要式身份验证。摘要式身份验证也要求用户输入账号名称和密码，但账号名称和密码都经过 MD5 算法处理，然后将处理后产生的散列随机数(hash)传送给 Web 服务器。采用这种方法时，Web 服务器必须是 Windows 域的成员服务器。

③ Windows 身份验证。集成 Windows 验证是一种安全的验证形式，它也需要用户输入用户账户和密码，但账户名和密码在通过网络发送前会经过散列处理，因此可以确保其安全性。Windows 身份验证方法有两种，分别是 Kerberos v5 验证和 NTLM，如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。

Windows 身份验证优先于基本身份验证，但它并不先提示用户输入用户名和密码，只有 Windows 身份验证失败后，浏览器才提示用户输入用户名和密码。虽然 Windows 身份验证非常安全，但是在通过 HTTP 代理连接时，Windows 身份验证不起作用，无法在代理服务器或其他防火墙应用程序后使用。因此，Windows 身份验证最适合企业 Intranet 环境。

用户可以基于 IP 地址或域名来允许或拒绝特定用户、计算机、计算机组或域访问该网站、目录或文件。在图 4-9 所示的“IP 地址和域名限制”选项组中单击“编辑”按钮，打开如图 4-11 所示的“IP 地址和域名限制”对话框。默认情况下，所有的计算机都被允许访问该网站。选中“授权访问”单选按钮，可以授权所有的计算机访问该网站，但在“下列除外”列表框中指定的计算机除外。要添加拒绝访问的计算机、计算机组或域，需单击“添加”按钮，打开如图 4-12 所示的“拒绝访问”对话框，在其中输入希望拒绝计算机的相应信息。输入后，单击“确定”按钮，被拒绝访问的计算机将出现在图 4-11 所示的“下列除外”列表框中。

图 4-11 “IP 地址和域名限制”对话框

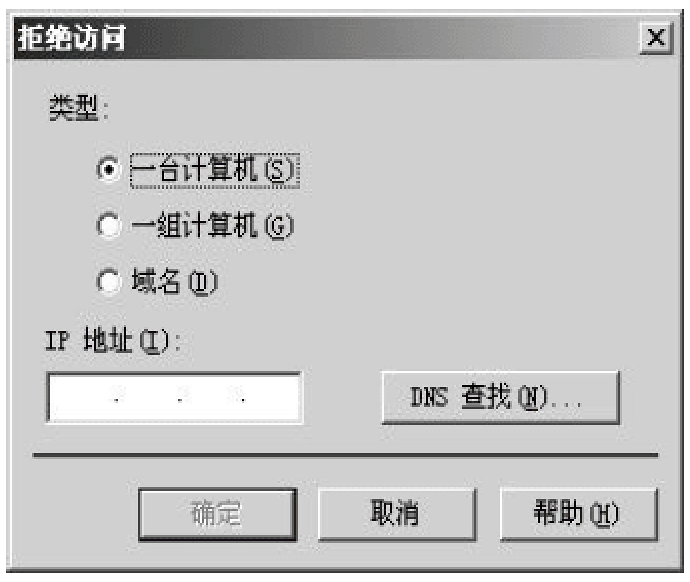


图 4-12 “拒绝访问”对话框

4.1.1.3 配置 FTP 服务器

Windows Server 2008 R2 中的 IIS 里内置 FTP 服务模块，安装比较简单。在 FTP 服务安装过程中，安装程序会自动创建一个“默认 FTP 站点”，可以直接修改该站点的属性来满足应用需求。为了更好地管理 FTP 服务器，需要对它进行适当的配置。

在 Internet 信息服务控制台下，右击“默认 FTP”选项，在弹出的快捷菜单中选择“属性”命令，弹出“默认 FTP 站点属性”对话框，如图 4-13 所示。对于“FTP 站点”“安全账户”“主目录”和“目录安全性”的设置基本上与 Web 站点相似，这里就不再赘述了。下面着重介绍“消息”选项卡中的相关设置，打开“消息”选项卡，如图 4-14 所示。

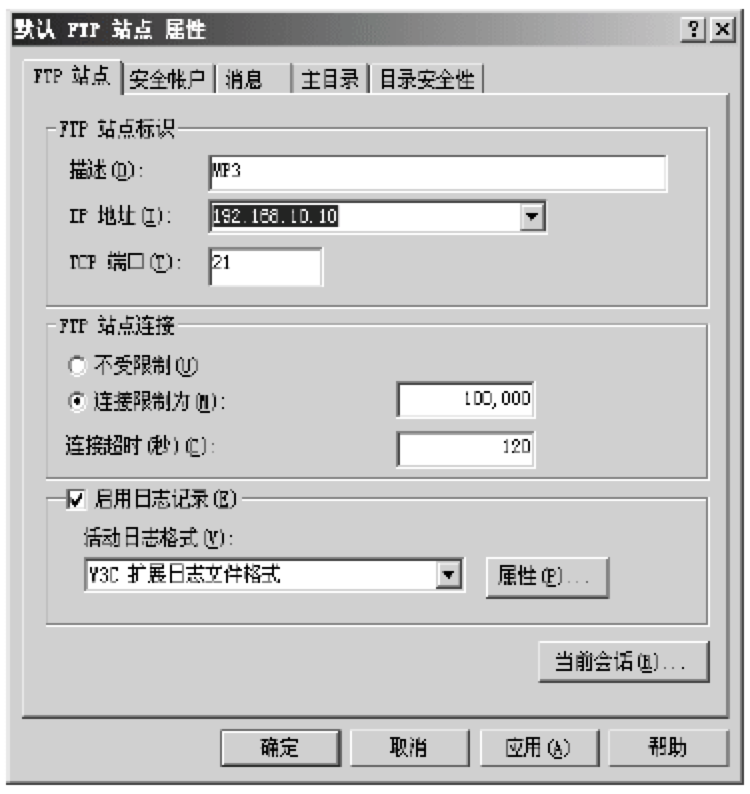


图 4-13　“默认 FTP 站点属性”对话框

图 4-14　“消息”选项卡

FTP 站点消息的相关设置如表 4-1 所示。

表 4-1　FTP 消息设置

配 置 项	说　明
标题	FTP 的站点名称，用户在登录 FTP 时显示的信息
欢迎	用户登录 FTP 时显示的信息
退出	当用户退出 FTP 时显示的信息
最大连接数	当 FTP 服务器超过最大连接人数时，给提出连接请求的客户机发送一条错误信息

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。在图 4-13 所示的“FTP 站点连接”选项组中，有 3 个选项可供选择。

- ◆ 不受限制：该选项允许同时发生的连接数将不受任何限制。
- ◆ 连接限制为：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。
- ◆ 连接超时：当某条 FTP 连接在一段时间内没有反应时，服务器就自动断开该连接。

4.1.2　典型例题分析

例 1　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2016 年下半年下午试题三)

【说明】

某公司的 IDC(互联网数据中心)服务器 Server1 采用 Windows Server 2003 操作系统，IP 地址为 172.16.145.128/24，为客户提供 Web 服务和 DNS 服务；配置了三个网站，域名分别为 www.companyl.com、www.company2.com 和 www.company3.com，其中 companyl 使用默

认端口。基于安全的考虑，不允许用户上传文件和浏览目录。company1.com、company2.com 和 Company3.com 对应的网站目录分别为 Company1-web、Company2-web 和 Company3-web，如图 4-15 所示。

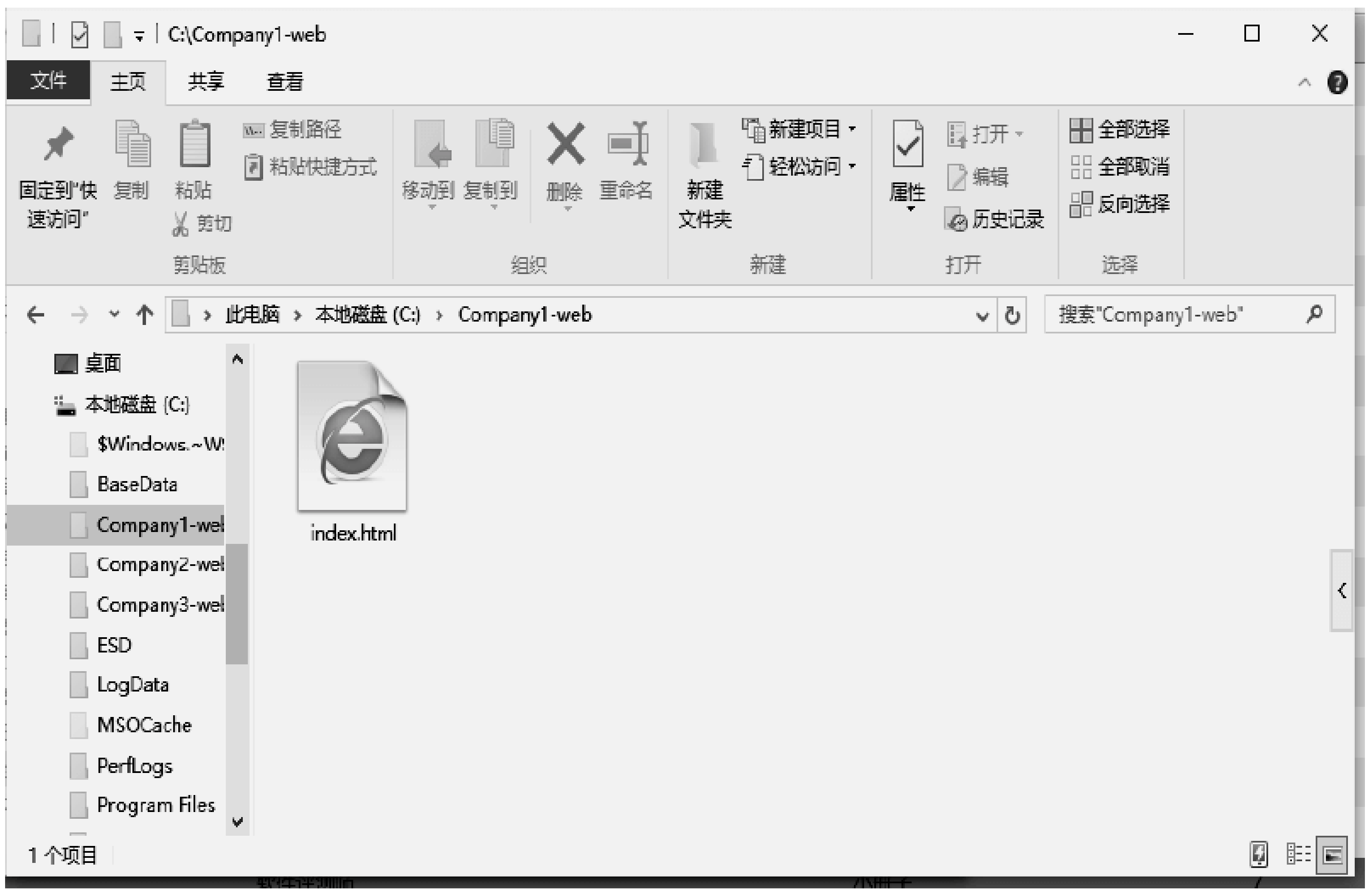


图 4-15　网站目录

【问题 1】(2 分，每空 1 分)

为安装 Web 服务和 DNS 服务，Server1 必须安装的组件有__(1)__、__(2)__。

(1)～(2)备选答案：

A. 网络服务　　B. 应用程序服务器　　C. 索引服务

D. 证书服务　　E. 远程终端

【问题 2】(4 分，每空 2 分)

在 IIS 中创建这三个网站时，在图 4-16 中勾选读取、__(3)__和执行，并在图 4-17 的“文档”选项卡中添加__(4)__为默认文档。

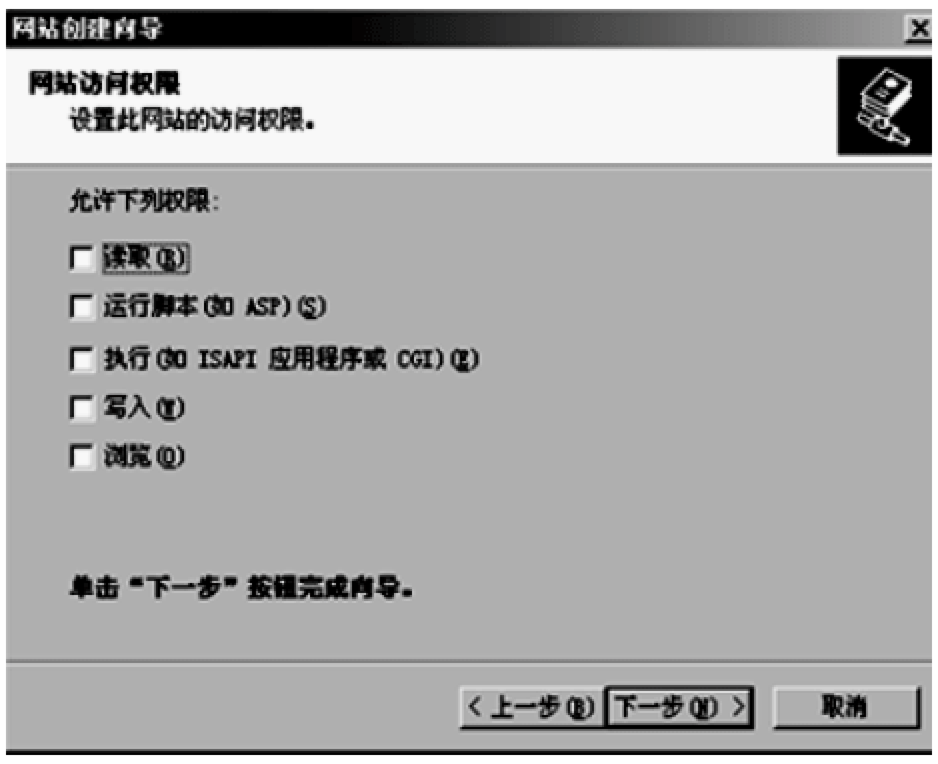


图 4-16　网站创建向导

图 4-17　“文档”选项卡

【问题 3】(6 分，每空 1 分)

1. 为了节省成本，公司决定在一台计算机上为多类用户提供服务。使用不同端口号来

区分不同网站，company1 使用默认端口__(5)__，company2 和 company3 的端口应在 1025 至__(6)__范围内任意选择，在访问 company2 或者 company3 时需在域名后添加对应端口号，使用__(7)__符号连接。设置完成后，管理员对网站进行了测试，测试结果如图 4-18 所示，原因是__(8)__。

图 4-18　测试结果

(8)备选答案：

A. IP 地址对应错误　　B. 未指明 company1 的端口

C. 未指明 company2 的端口　　D. 主机头设置错误

2. 为便于用户访问，管理员决定采用不同主机头值的方法为用户提供服务，需在 DNS 服务中正向查找区域为三个网站域名分别添加__(9)__记录。网站 company2 的主机头值应设置为__(10)__。

【问题 4】(8 分，每空 2 分)

如果随着 company1 网站访问量的不断增加，公司为 company1 设立了多台服务器。下面是不同用户 ping 网站 www. company1.com 后返回的 IP 地址及响应状况，如图 4-19 所示。

```
Microsoft Windows [版本 5.2.3790]
 (c) 版权所有 1985-2003 Microsoft Corp.

C:\Users>ping www.company1.com
Pinging company1.wscache.ourglb0.com [172.16.145.192] with 32 bytes of data:

Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57
Reply from 172.16.145.192:bytes=32 time=11ms TTL=57

Ping statistics for 172.16.145.192:
      Packets:Sent=4, Received=4, Lost=0<0% loss>,
Approximate round trip times in milli-seconds:
      Mininum=11ms, Maxinum=15ms, Average=13ms
```

```
Microsoft Windows [版本 10.0.10586]
 (c) 版权所有 2015 Microsoft Corporation.

C:\Users>ping www.company1.com
Pinging company1.wscache.ourglb0.com [172.16.145.193] with 32 bytes of data:

Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57
Reply from 172.16.145.193:bytes=32 time=11ms TTL=57

Ping statistics for 172.16.145.193:
      Packets:Sent=4, Received=4, Lost=0<0% loss>,
Approximate round trip times in milli-seconds:
      Mininum=5ms, Maxinum=8ms, Average=6ms
```

图 4-19　响应状况

从图 4-19 可以看出，域名 ww.company1.com 对应了多个 IP 地址，说明在图 4-20 所示的 DNS 属性中启用了__(11)__功能。

如果在图 4-20 中勾选了“启用网络掩码排序”后，当存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 的网络掩码匹配度，按照__(12)__原则来应答客户端的解析请求。如果勾选了“禁用递归”，这时 DNS 服务器仅采用__(13)__查询模式。当同时启用了网络掩码排序和循环功能时，__(14)__优先级较高。

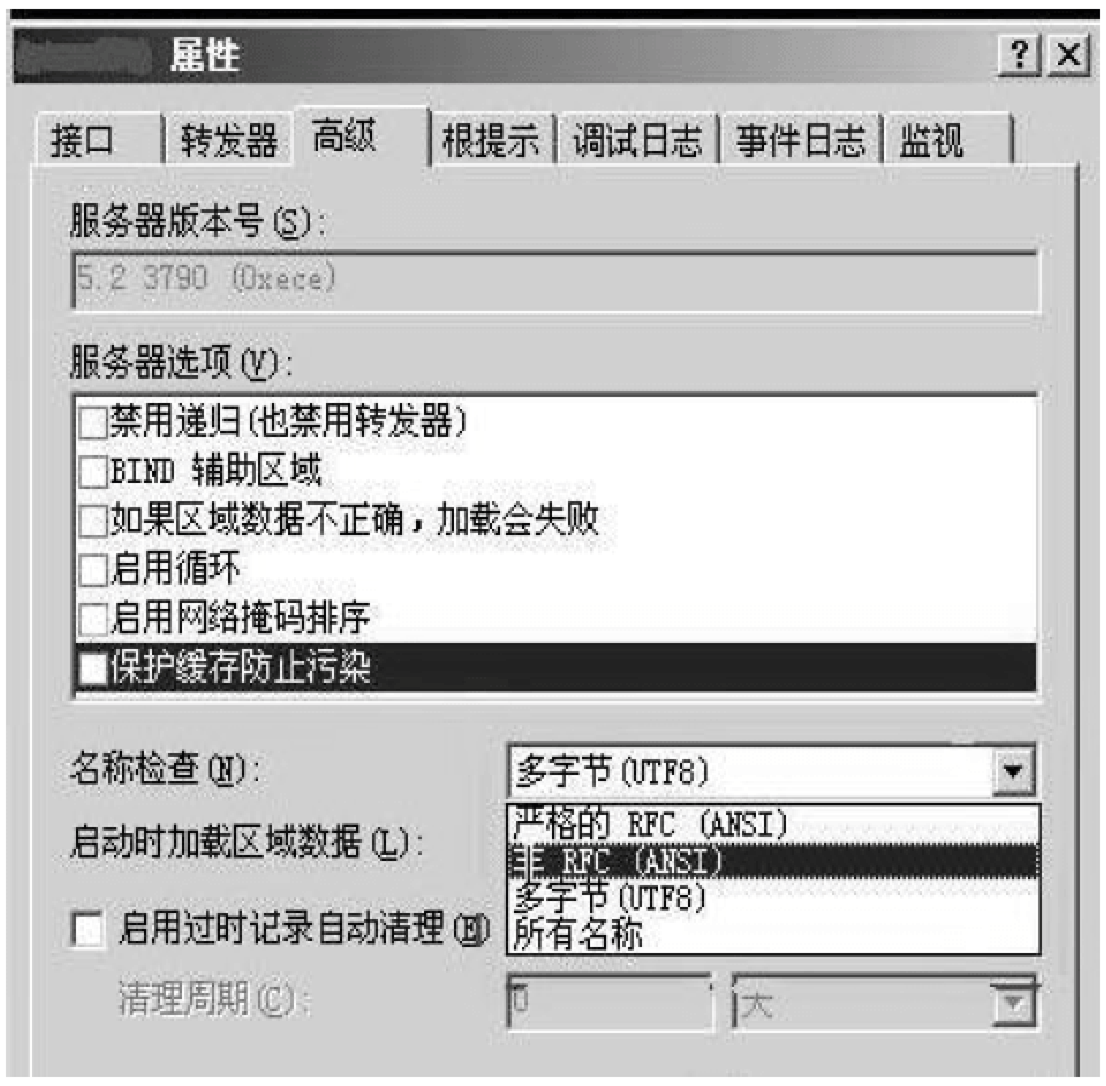


图 4-20　DNS 属性

(14)备选答案：

A. 循环　　　　B. 网络掩码排序

答案：

【问题 1】(1) A　(2) B (答案顺序可互换)

【问题 2】(3) 运行脚本(如 ASP)(S)　(4) index.html

【问题 3】(5) 80　(6) 65535　(7) :　(8) C　(9) A(DNS 的 A 记录)

(10) www.company2.com

【问题 4】(11) 循环　(12) 掩码接近度匹配对访问者实现的本地子网优先级排序

(13) 迭代　(14) B

解析：

【问题 1】出于对服务器安全性的着想，微软取消了安装操作系统时默认安装相关 Windows 组件的做法，因此安装 Web 服务和 DNS 服务，Server1 需要分别在“Windows 组件向导”中选中“应用服务器”和“网络服务”复选框，而后才能进行相关配置。

【问题 2】从题目中“不允许用户上传文件和浏览目录”可见访问权限设置中，不能选择“写入”和“浏览”权限。

默认文档：它是指在访问您网站的时候自动定位的一个首先访问页面文件。本题中的网站主目录中只有一个文件 index.html，而“文档”选项卡中无此文档，所以需要手工添加。

【问题 3】Web 服务的默认端口是 80，在一台计算机上建立多站点，可以使用不同 IP 地址、不同主机头、不同端口号三种方式，其中：采用端口号区分不同站点。对于非标准端口，在访问时需要在域名或 IP 地址后面加上“：端口号”，如 www. company2.com: 8080。用不同主机头值的方法时，需要在 DNS 中为每个网站的域名添加主机记录，对于 IP 地址是同一个地址，每个站点的主机头设置为这个站点的完整域名，如网站 company2 的主机头值设置为：www.company2.com。采用主机头区分站点在访问时不能通过 IP 地址，只能通过域名的方式访问。

【问题 4】DNS 轮询就是指 DNS 服务器将域名解析请求按照 A 记录的顺序，逐一分配到不同的 IP 上，同时在一定程度上也实现了简单的负载均衡。

网络掩码排序可以根据本地子网优先级来判断 DNS 地址和客户端是否在同一个网段或者离得比较近，然后优先返回较近的服务器的地址。

关于本地子网优先级:

当集群中的服务器不在同一网段时，默认情况下，当客户机查询解析映射到多个 IP 地址的主机名时，DNS 服务使用本地子网优先排序作为给出同一网络上首选 IP 地址的方法。此功能要求客户应用程序尝试使用连接可用的最近(一般是最快的)IP 地址连接至主机。

DNS 服务按以下方式使用本地子网优先级。

① DNS 服务确定是否需要本地子网的优先级排序查询响应。

如果有多个地址资源记录与要查询的主机名匹配，则 DNS 服务可按其子网位置重新对记录进行排序。如果查询的主机名只与一个地址资源记录匹配，或者客户机的 IP 网络地址与多重资源记录响应列表上的任何映射地址的 IP 网络地址匹配，则不需要进行优先排列。

② 对于匹配响应列表中的每一个资源记录，DNS 服务决定了哪些记录(如果有)与查询客户机的子网位置匹配。

③ DNS 服务重新对响应列表进行排序，以便将与发出请求的客户机的本地子网匹配的主机地址资源记录排在响应列表中的第一位。

④ 按子网的顺序进行优先级排序后，响应列表将返回给发出请求的客户机。

DNS 属性中启用“循环”功能后，同一个域名可以对应多个 IP 地址。当启用“网络掩码排序”功能后，如果存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 地址的网络掩码匹配度，按照最长匹配的原则来应答客户端的解析请求。

DNS 查询模式有递归查询和迭代查询，当在 DNS 属性中勾选了“禁用递归”时，DNS 服务器就会采用迭代模式。如果同时启用了“网络掩码排序”和“循环”功能时，网络掩码排序的优先级较高。

DNS 查询分为递归和迭代两种模式，本题中禁用递归，则必然是使用迭代查询模式。

例 2　【说明】(2015 年下半年下午试题三)

某企业采用 Windows Server 2003 配置了 Web、FTP 和邮件服务。

【问题 1】(4 分)

Web 的配置如图 4-21 和图 4-22 所示。

图 4-21　“主目录”选项卡

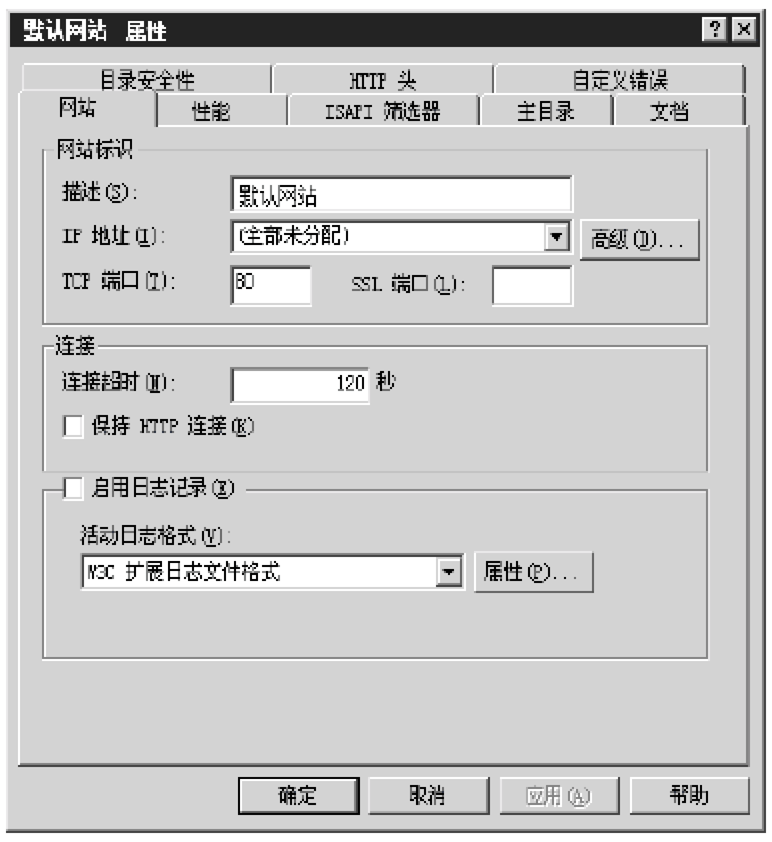


图 4-22　“网站”选项卡

1. 如果要记录用户访问历史，需__(1)__。

(1)备选答案

A. 同时勾选图 4-21 中“写入”复选框和图 4-22 中“启用日志记录”复选框

B. 同时勾选图 4-21 中“记录访问”复选框和图 4-22 中“启用日志记录”复选框

C. 同时勾选图 4-21 中“记录访问”复选框和“索引资源”复选框

D. 同时勾选图 4-21 中“记录访问”复选框和图 4-22 中“保持 HTTP 连接”复选框

2. 在图 4-22 所示的 4 种活动日志格式中，需要提供用户名和密码的是__(2)__。

【问题 2】(4 分)

根据图 4-21 判断正误。(正确的答“对”，错误的答“错”)

A. 勾选“读取”是指禁止客户下载网页文件及其他文件。__(3)__

B. 不勾选“写入”是指禁止客户以 HTTP 方式向服务器写入信息。__(4)__

C. 勾选“目录浏览”是指当客户请求的文件不存在时，将显示服务器上的文件列表。__(5)__

D. 当网页文件是 CGI 文件时，“执行权限”中选择“纯脚本”。__(6)__

【问题 3】(6 分)

FTP 的配置如图 4-23 所示。

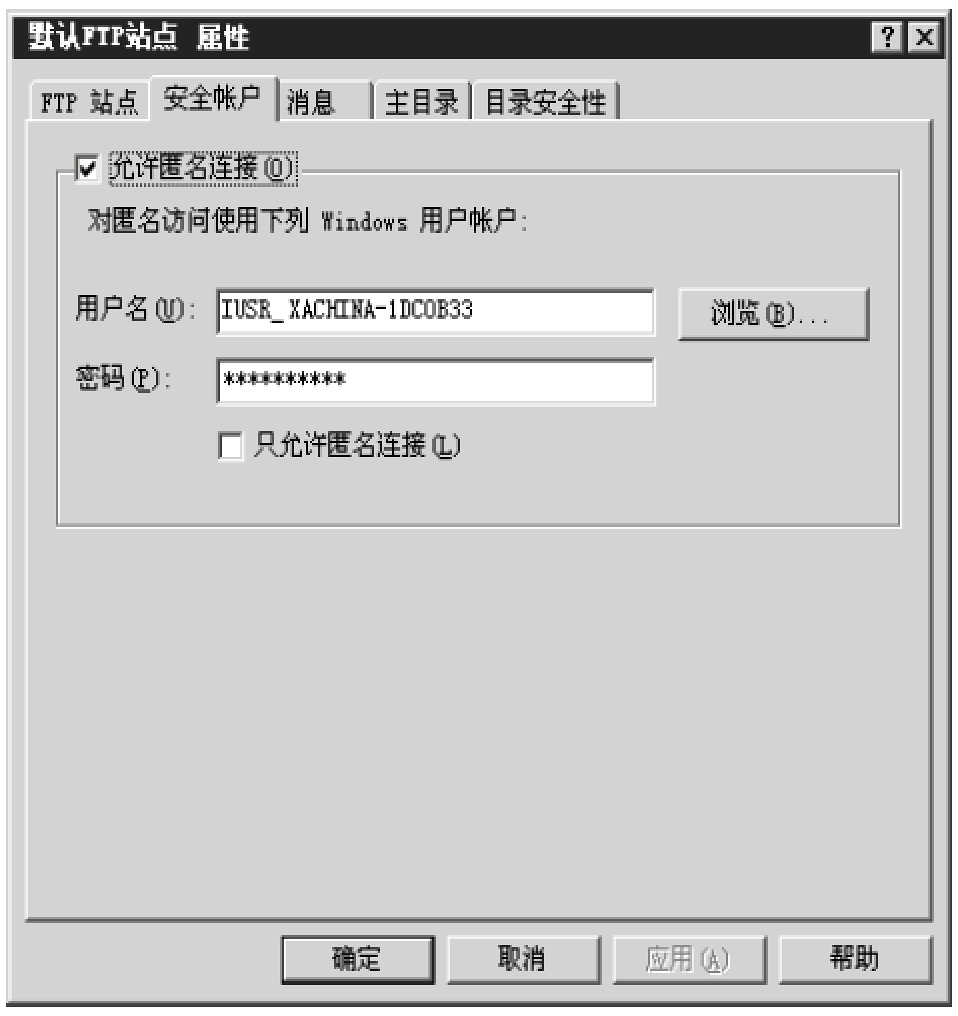


图 4-23 “安全账户”选项卡

匿名用户的权限与在“本地用户和组”的权限__(7)__，FTP 可以设置__(8)__虚拟目录。FTP 服务器可以通过__(9)__访问。

(9)备选答案：

A. DOS、客户端方式

B. 客户端、浏览器方式

C. DOS、浏览器、客户端方式

【问题 4】(6 分)

邮件服务器的配置如图 4-24 所示。

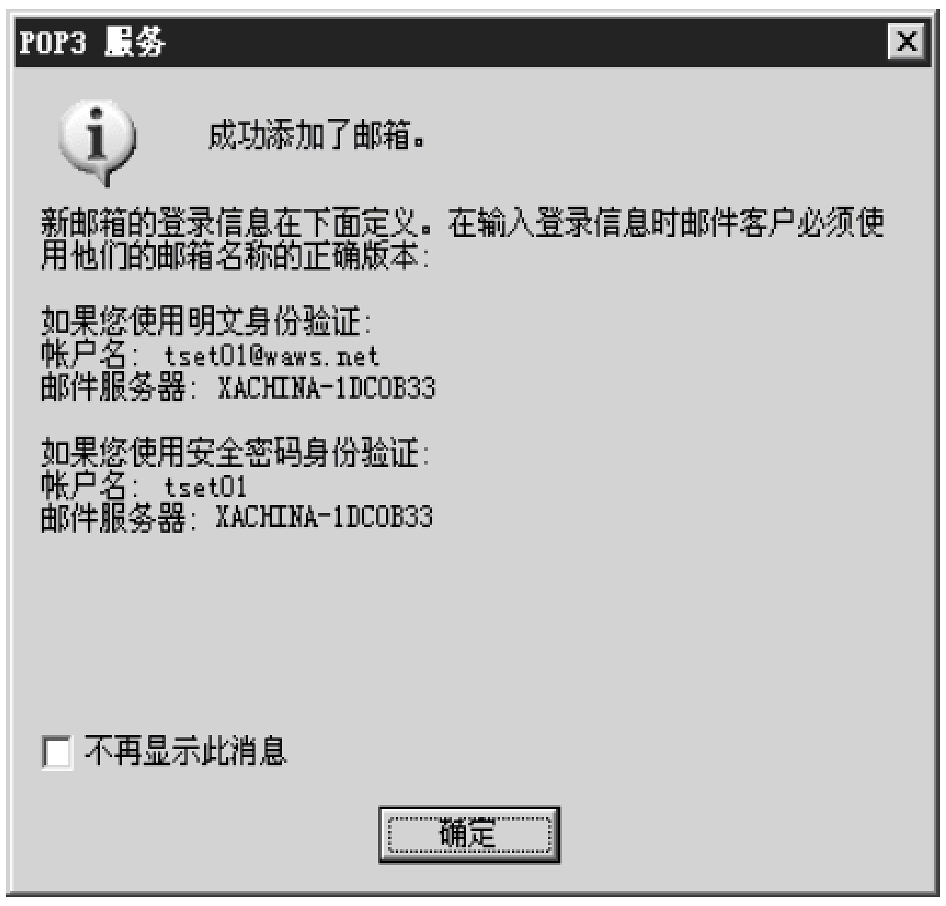


图 4-24　“POP3 服务”对话框

若图 4-24 所示 waws.net 域已经在 Internet 上注册，那么在 DNS 服务器中应配置邮件服务器的 (10) 记录。POP3 是 (11) 邮件协议，配置 POP3 服务器的步骤包含 (12) (多选)。

(11)备选答案：

A. 接收　　B. 发送　　C. 存储　　D. 转发

(12)备选答案：

A. 创建邮件域　　B. 设置服务器最大连接数

C. 安装 POP3 组件　　D. 添加邮箱

答案：

【问题 1】(1) B　(2) ODBC 日志记录

【问题 2】(3) 错　(4) 对　(5) 对　(6) 错

【问题 3】(7) 相同　(8) 站点　(9) C

【问题 4】(10) MX　(11) A　(12) C、A、D

解析：

【问题 1】

记录访问：在日志文件中记录对网站的访问。需要勾选“记录访问”和“启用日志记录”复选框。

在 4 种活动日志格式中，只有 ODBC 日志记录需要连接数据库，需要提供用户名和密码。

【问题 2】

读取：由于网站主要是供用户浏览的，一般指需要选择“读取”即可。

写入：客户以 HTTP 方式向服务器写入内容。

目录浏览：客户可以查看服务器上文件的目录结构。

CGI 是外部应用程序(CGI 程序)与 Web 服务器之间的接口标准。当网页是 CGI 时候，执行选项改成脚本和可执行程序。

【问题 3】

匿名用户的权限和“本地用户和组”的权限相同，FTP 设置站点虚拟目录。FTP 服务器可以通过 DOS、浏览器、客户端方式访问。

【问题 4】

MX 记录是用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当收件人为“user@csai.com”时，系统将对“csai.com”进行 DNS 中的 MX 记录解析。如果 MX 记录存在，系统就根据 MX 记录的优先级，将邮件转发到与该 MX 相应的邮件服务器上。

POP3 是电子邮件接收协议，配置 POP3 服务器的步骤包括安装 POP 组件、创建邮件域、添加邮箱。

例 3 【说明】(2015 年上半年下午试题三)

某企业采用 Windows Server 2003 配置了共享打印、FTP 和 DHCP 服务。

【问题 1】(8 分)

1. Internet 共享打印使用的协议是__(1)__。(1 分)

(1)备选答案：

A. PPI　　B. IPP　　C. TCP　　D. IP

2. Internet 共享打印配置完成后，需在如图 4-25 所示的“Web 服务扩展”选项界面中将 Active Server Pages 设置为“允许”，其目的是__(2)__。(2 分)

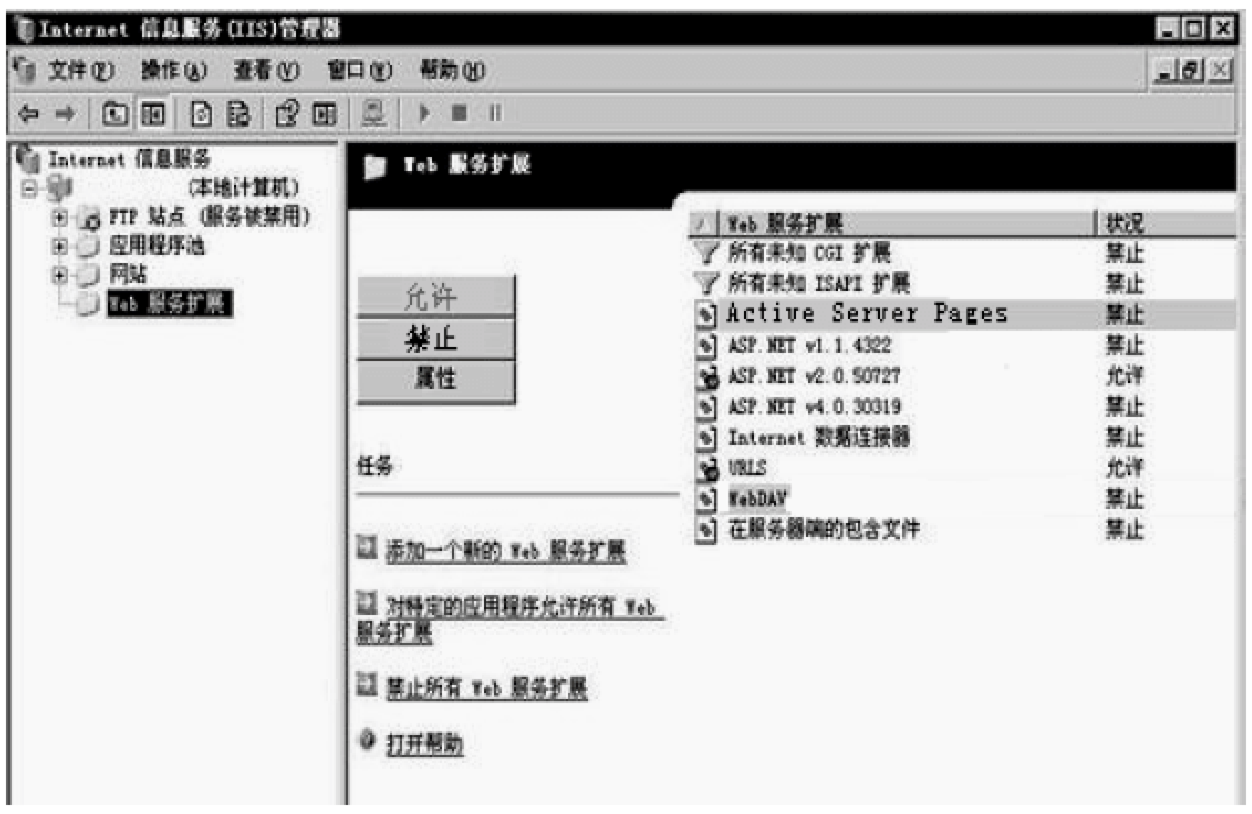


图 4-25　“Web 服务扩展”选项界面

3. 检验 Internet 打印服务是否安装正确的方法是在 Web 浏览器的地址栏输入 URL 是__(3)__。(2 分)

(3)备选答案：

A. HTTP: //127.0.0.1/PRINTERS　　B. FTP: //127.0.0.1/PRINTERS

C. HTTP: //PRINTERS　　D. FTP: //PRINTERS

4. 使用 Internet 共享打印流程为 6 个步骤：

① 在终端上输入打印设备的 URL

② 服务器向用户显示打印机状态信息

③ 客户端向打印服务器发送身份验证信息

④ 用户把要打印的文件发送到打印服务器

⑤ 打印服务器生成一个 cabinet 文件，下载到客户端

⑥ 通过 Internet 把 HTTP 请求发送到打印服务器

对以上步骤进行正确的排序__(4)__。(3 分)

【问题 2】 (8 分)

FTP 的配置如图 4-26 和图 4-27 所示。

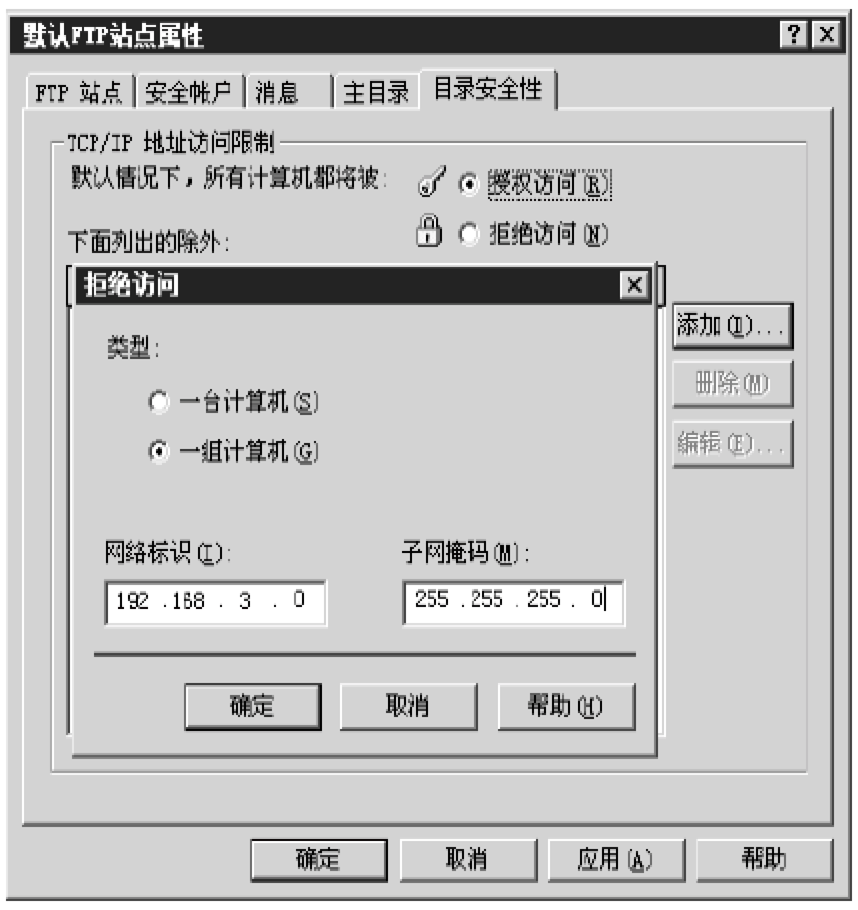


图 4-26　“目录安全性”选项卡

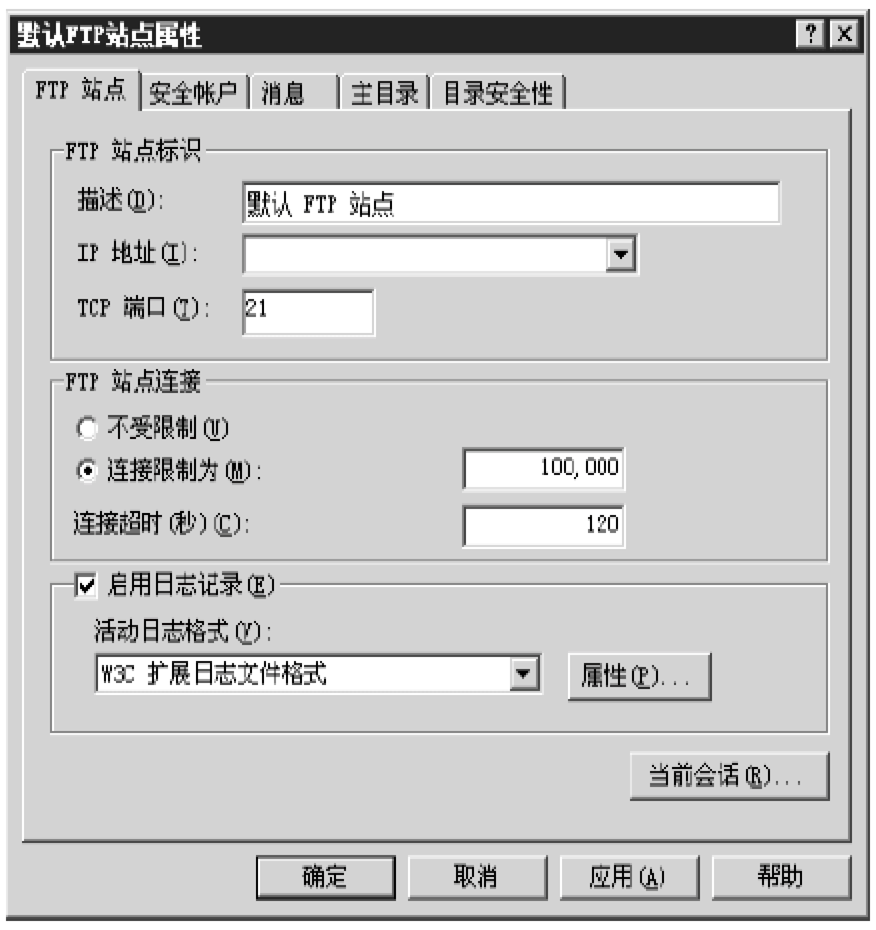


图 4-27　“FTP 站点”选项卡

1. 默认情况下，用户登录 FTP 服务器时，服务器端建立的 TCP 端口号为__(5)__。
2. 如果只允许一台主机访问 FTP 服务器，参考图 4-26 给出具体的操作步骤__(6)__。
3. 参考图 4-27，在一台服务器上搭建多个 FTP 站点的方法是__(7)__。
4. 如单击图 4-27 中“当前会话”按钮，显示的信息是__(8)__。

【问题 3】 (4 分)

DHCP 的配置如图 4-28 和图 4-29 所示。

图 4-28　“常规”选项卡

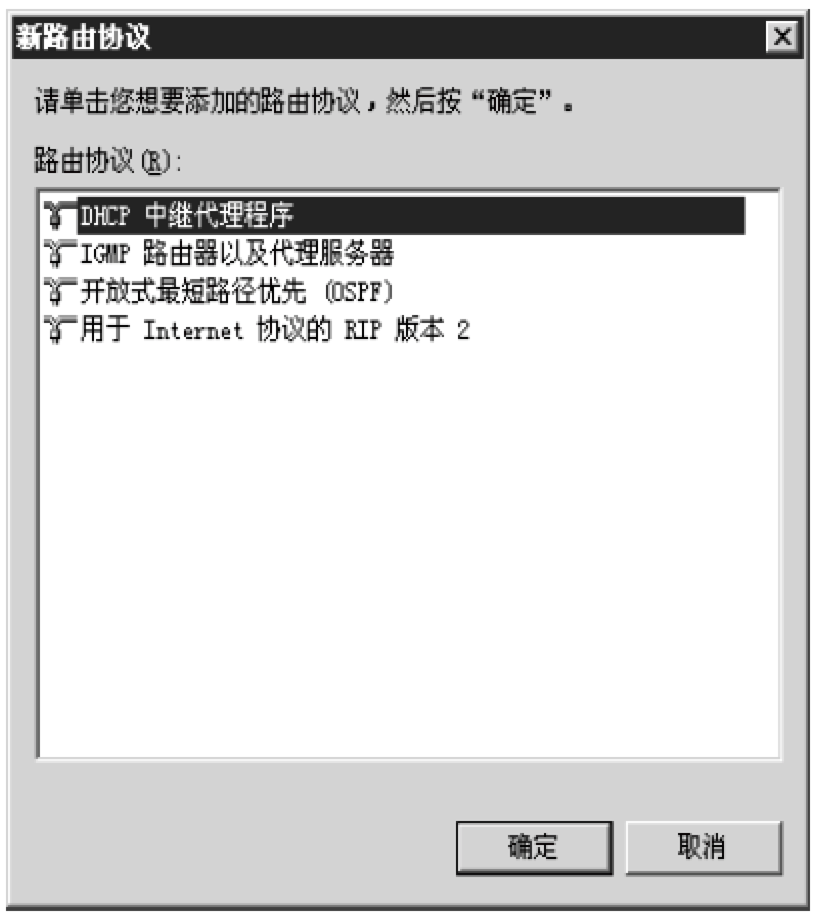


图 4-29　“新路由协议”对话框

1. 图 4-28 中填入的 IP 地址是__(9)__。
2. 图 4-29 中配置 DHCP 中继代理程序，可以实现__(10)__。

(9)备选答案：

A. 分配给客户端的 IP 地址

B. 默认网关的 IP 地址

C. DHCP 服务器的 IP 地址

(10)备选答案：

A. 使普通客户机获取 IP 等信息

B. 跨网段的地址分配

C. 特定用户组访问特定网络

答案：

【问题 1】

(1) B　(2) 允许运行 Internet 打印服务的 ASP 脚本　(3) A　(4) ①⑥③②⑤④

【问题 2】

(5) 21

(6) 选中“拒绝访问”，添加允许计算机的 IP 地址

(7) 不同的 IP 地址或相同的 IP、不同的 TCP 端口

(8) 连接的客户端会话信息

【问题 3】

(9) B　(10) B

解析：

【问题 1】

IPP(Internet 打印协议)侦听服务提供了一个 IPP 网络协议服务，该服务为打印客户机系统提供一种与运行侦听程序的系统上的打印服务进行交互的方法。此侦听程序实现了服务器端 IPP 协议支持，其中包括一组广泛的标准操作和属性。

开启 Active Server Pages 服务扩展，以便允许服务器运行 Internet 打印服务的 ASP 脚本文件。

通过 Web 访问 Internet 打印服务器的方法为：HTTP: //127.0.0.1/PRINTERS。

Internet 打印流程如下。

(1) 用户输入打印设备的 URL(统一资源定位符)，通过 Internet 连接到打印服务器。

(2) HTTP 请求通过 Internet 发送到打印服务器。

(3) 打印服务器要求客户端提供身份验证信息。这样能够确保只有经过授权的用户才能在打印服务器上打印文件。

(4) 当用户获得授权可以访问打印服务器后，服务器使用活动服务器页(Active Server Pages，ASP)向用户显示状态信息，其中包括有关当前空闲打印机的信息。

(5) 当用户连接 Internet 打印网页上的任何打印机时，客户端计算机首先尝试在本地寻找该打印机的驱动程序。如果没有找到适合的驱动程序，打印服务器将会生成一个 cabinet 文件(.cab 文件，又称为 Setup 文件)，其中包含正确的打印机驱动程序文件。打印服务器把.cab 文件下载到客户端计算机上。客户端计算机提示用户允许下载该.cab 文件。

(6) 当用户连接到 Internet 打印机后，他们可以使用 Internet 打印协议(Internet Printing Protocol，IPP)把文件发送到打印服务器。

【问题 2】

FTP 使用的 TCP 端口号为 21。

“目录安全性”选项卡中，只允许单台主机访问，可以选中“拒绝所有”，然后添加主机的 IP 地址。

搭建多个 FTP 站点的方式是：不同 IP 地址或相同的 IP、不同的端口号。

“当前会话”中，显示了连接到 FTP 服务器的客户端信息。

【问题 3】

配置 DHCP 服务器选项时，003 路由器设置分配给客户端的网关地址。通过 DHCP 中继代理，可以实现跨网段的地址分配。

4.1.3　同步练习

1. 【说明】(2014 年下半年下午试题二)

某中学为两个学生课外兴趣小组提供了建立网站的软硬件环境。网站环境的基本配置方案如下。

(1)　两个网站配置在同一台服务器上，网站服务由 Windows 2003 环境下的 IIS 6.0 提供。

(2)　网站的管理通过 Windows 2003 的远程桌面实现，并启用 Windows 2003 的防火墙组件。

(3)　为兴趣小组建立各自独立的文件夹作为上传目录和网站的主目录，对用户使用磁盘空间大小进行了设定。

(4)　通过不同的域名分别访问课外兴趣小组各自的网站。

按照方案，学校的网络工程师安装了 Windows 2003 服务器，使用 IIS 6.0 建立 Web 和 FTP 服务器，配置了远程桌面管理、防火墙，在服务器上为两个课外兴趣小组分配了不同的用户名，进行了初步的权限配置。

【问题 1】(4 分)

Windows 2003 远程桌面服务的默认端口是__(1)__，对外提供服务使用__(2)__协议。在图 4-30 中，若要拒绝外部设备 ping 服务器，在防火墙的 ICMP 配置界面上应该如何操作？

【问题 2】(4 分)

1. 在图 4-31 中，“Web 服务扩展”选项界面中“所有未知 CGI 扩展禁止”的含义是什么？

2. 在图 4-31 中，如何配置 Web 服务扩展，网站才能提供对 asp.net 或 ASP 程序的支持。

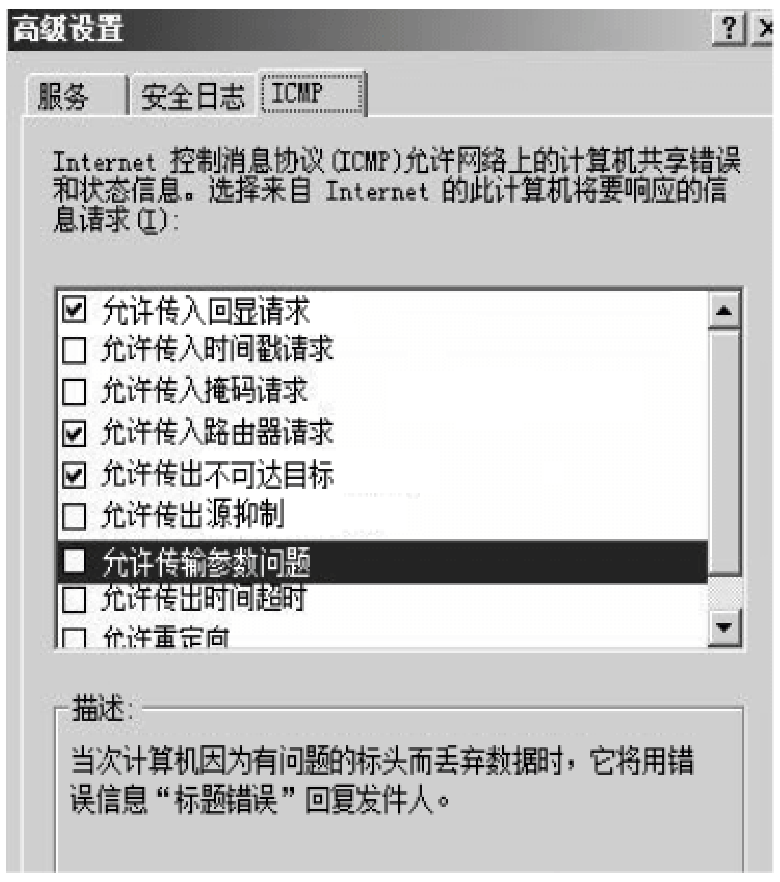


图 4-30　“高级设置”对话框

图 4-31　“Web 服务扩展”选项界面

【问题 3】(5 分)

在图 4-31 中，选择 IIS 管理器中的“FTP 站点”→“新建”→“虚拟目录”，分别设置 FTP 用户与 (3) 、 (4) 的对应关系。

由于 IIS 内置的 FTP 服务不支持 (5) ，所以 FTP 用户密码是以明文方式在网络上传输，安全性较弱。

【问题 4】(4 分)

在 IIS 6.0 中，每个 Web 站点都具有唯一的、由三部分组成的标识符，用来接收和响应请求，分别是 (6) 、 (7) 和 (8) 。网络工程师通过单击“网站属性”→“网站”→“高级选项”，通过添加 (9) 的方式在一个 IP 地址上建立多个网站。

【问题 5】(3 分)

在 (10) 文件系统下，为了预防用户无限制地使用磁盘空间可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是 (11) 和 (12) 。

2. 【说明】(2014 年上半年下午试题二)

某公司采用 Windows Server 2003 操作系统搭建该公司的企业网站，要求用户在浏览器地址必须输入 https://www.gqngsi.com/index.html 或 https://117.112.89.67/index.html 来访问该公司的网站。其中，index.html 文件存放在网站服务器 E:\gsdata 目录中。在服务器上安装完成 IIS 6.0 后，“默认网站属性”对话框“网站”“主目录”选项卡分别如图 4-32 和图 4-33 所示。

图 4-32 “网站”选项卡

图 4-33 “主目录”选项卡

【问题 1】(4 分)

1. 按照题目说明，图 4-32 中的“IP 地址”文本框中的内容为 (1) ；“SSL 端口”文本框内容为 (2) 。

2. 在图 4-33 中，“本地路径”文本框中的内容为 (3) ；同时要保障用户通过题目要求的方式来访问网址，必须至少勾选 (4) 复选框。

(4)备选答案：

A. 脚本资源访问　　B. 读取　　C. 写入　　D. 目录浏览

【问题 2】(6 分)

1. 配置该网站时，要在如图 4-34 所示“目录安全性”选项卡中单击“服务器证书”按钮来获取服务器证书，其中获取服务器证书的步骤顺序如下：①生产证书请求文件；②__(5)__；③从 CA 导出证书文件；④在 IIS 服务器上导入安装文件。

2. 配置完成后，当用户登录该网站时，通过验证 CA 的签名来确认数字证书的有效性，从而__(6)__，CA 颁发给 Web 网站的数字证书不包括__(7)__。

(6)~(7)备选答案：

(6) A. 验证网站的真伪　　B. 判断用户的权限

C. 加密发送服务器的数据　　D. 解密所接收的客户端数据

(7) A. 证书的有效期　　B. 网站的公钥

C. 证书的序列号　　D. 网站的私钥

【问题 3】(2 分)

配置该网站时，在图 4-34 的对话框中单击“安全通信”选项组中的“编辑”按钮，弹出如图 4-35 所示对话框。按题目要求，客户端浏览器只能通过 HTTPS 方式访问服务器，此时应勾选图 4-35 中的__(8)__框，如果要求客户端和服务器进行双向认证，此时应勾选图 4-35 中的__(9)__框。

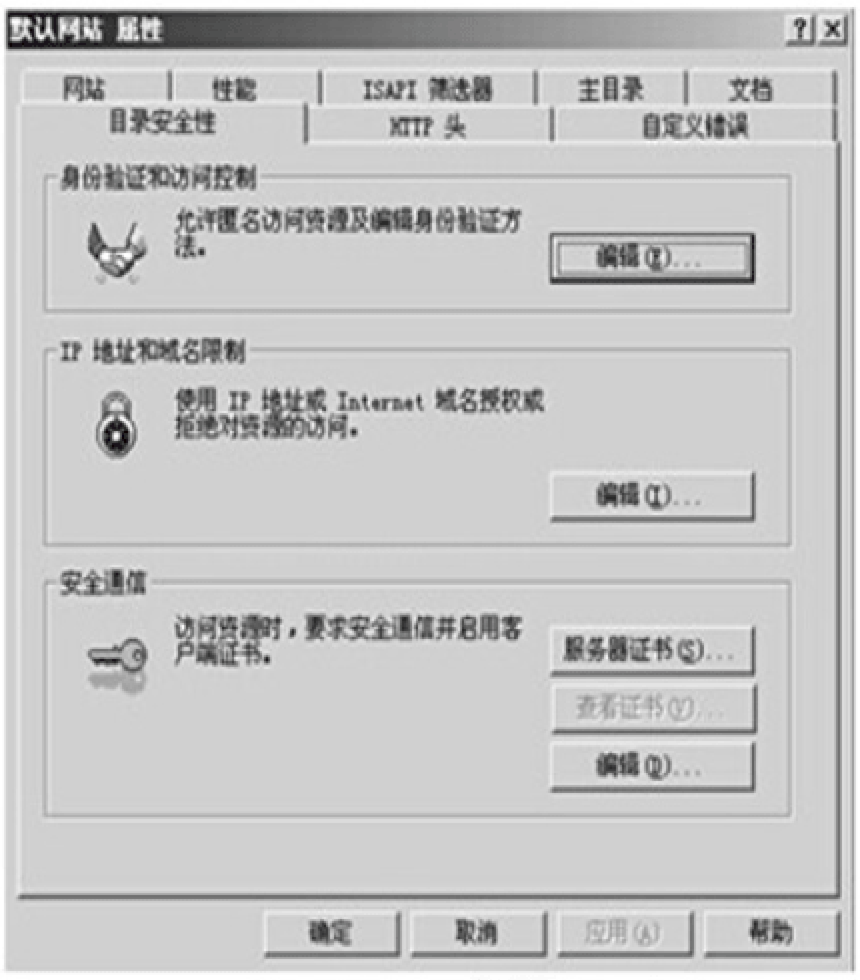


图 4-34　“目录安全性”选项卡

图 4-35　“安全通道”对话框

【问题 4】(2 分)

HTTPS 用于在客户计算机和服务器之间提供安全通信，广泛用于因特网上安全敏感的应用，例如__(10)__应用。

HTTPS 使用安全套接子层(SSL)进行信息交换。SSL 目前版本是 3.0，被 IETF 定义在 RFC 6101 中。IETF 对 SSL 进行升级后的继任者是__(11)__。

(10)备选答案：

A. 网络聊天　　B. 网络视频　　C. 网上交易　　D. 网络下载

【问题 5】(1 分)

使用 HTTPS 能不能确保服务器自身安全？

4.1.4 同步练习参考答案

1. 答案：

【问题 1】

(1) 3389　(2) RDP

取消勾选“允许传入回显请求”

【问题 2】

1. 除非明确允许一个应用在 IIS 6.0 上允许，否则就禁止运行，提高安全性。

2. Active Server Pages 修改为允许。

【问题 3】

(3) xiaozu-a　(4) xiaozu-b　(5) SSL

【问题 4】

(6) IP 地址　(7) 端口　(8) 域名　(9) 主机头

【问题 5】

(10) NTFS　(11) 磁盘配额限制　(12) 磁盘配额警告级别

解析：

【问题 1】Windows 2003 远程桌面服务的默认端口是 3389，对外提供服务使用 RDP 协议(远程显示协议)。拒绝外部设备 ping 服务器，也就是不允许传入回显请求。

【问题 2】如果选择允许所有通用网关接口(CGI)在 Web 服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在 IIS 6.0 上运行，否则它就不能运行。

要想网站提供对 ASP.NET 或 ASP 程序的支持，必须增加 ASP.NET 模块(启用 ASP.NET 的服务扩展项)。将 Active Server Pages 配置为“允许”，IIS 6.0 即可提供对 ASP 支持。

【问题 3】FTP (File Transfer Protocol, FTP)是 TCP/IP 网络上两台计算机传送文件的协议，FTP 是在 TCP/IP 网络和 Internet 上最早使用的协议之一，它属于网络协议的应用层。FTP 客户机可以给服务器发出命令来下载文件、上传文件、创建或改变服务器上的目录，FTP 的默认端口是 21。由于 IIS 中的 FTP 服务不支持安全套接层(SSL)上的 FTP，因此，如果要保证通信的安全性，同时又需要使用 FTP 作为传输协议(相对于在 SSL 上使用 WebDAV 而言)，可以考虑在加密通道(如虚拟专用网络)上使用 FTP，此类加密通道通过点对点隧道协议或 IPSec 保证安全性。

【问题 4】IIS 是一种 Web(网页)服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。IIS6.0 增强了安全性，为了尽量减少系统被攻击的危险，在默认情况下，IIS 6.0 是不会被安装在 Win 2003 中的，管理员需要手动进行安装，IIS 6.0 在被锁定状态中只为静态内容(.htm，.jpg，.bmp 等)提供服务，通过网络服务扩展节点，网站管理员可根据企业的需求起用或禁止 IIS 功能。

【问题 5】NTFS 文件系统可以进行磁盘配额管理。磁盘配额就是管理员可以为用户所能使用的磁盘空间进行配额限制，每一个用户只能使用最大配额范围内的磁盘空间。设置

磁盘配额后，可以对每一个用户的磁盘使用情况进行跟踪和控制，通过监测可以标识出超过配额报警阈值和配额限制的用户，从而采取相应的措施。磁盘配额管理功能的提供，使得管理员可以方便合理地为用户分配存储资源，避免由于磁盘空间使用的失控可能造成的系统崩溃，提高了系统的安全性。

2. **答案：**

【问题 1】

(1) 117.112.89.67　(2) 443　(3) E:\gsdata　(4) B 或读取

【问题 2】

(5) 提交证书申请　(6) A 或验证网站的真伪　(7) D 或网站的私钥

【问题 3】

(8) “要求安全通道(SSL) ”　(9) “要求客户端证书”

【问题 4】

(10) C 或网上交易　(11) TLS

【问题 5】不能

解析：

【问题 1】

1. 题干中明确说明可以通过 https: //117.112.89.57/index.html 访问公司网站，则在图 4-32 中“网站”选项卡“IP 地址”文本框输入的 IP 址为 117.112.89.67。

SSL(Secure Sockets Layer，安全套接层)及其继任者安全传输层(Transport Layer Security，TLS)是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL 在传输层对网路连接进行加密。该协议结合 HTTP 构成 HTTPS 协议，HTTPS 协议是 HTTP 的安全升级版，该协议基于 TCP 443 端口。

2. 题干中明确说明 index.html 文件放在网站服务器 E:\gsdata 目录中，图 4-33“本地路径”文本框应填入 E:\gsdata。对于一个网站而言，可以通过 IP 或域名的方式访问，在 4-33 中至少应该开启“读取”权限，否则此网站是不能访问的。

【问题 2】

为了保证网站与客户交互过程中的安全性，可以为网站服务器向 CA 申请服务器证书，证书上绑定了服务器的 ID 和公钥，用户访问此网站时，下载服务器证书，并利用服务器上的公钥加密交互信息，以达到机密性的要求。服务器向 CA 申请证书的过程为：

① 生成证书请求文件。

② 提交证书申请。

③ 从 CA 导出证书文件。

④ 在 IIS 服务器上导入并安装证书。

用户访问网站服务器时，下载服务器证书首先通过证书上 CA 的签名鉴别该证书的合法性，就好像日常生活中办理宾馆入住要先提交身份证一样。确认该服务器证书合法之后，表示客户端信任了该证书的主体(网站服务器)。X.509 标准规定了证书包含版本、序列号、签名算法标识符、签发人签名、有效期、主体名、主体公钥信息等，但不包含证书主体的私钥。

【问题 3】

客户端只能通过 HTTPS 方式访问网站服务器，则应该开启 SSL 功能，通过勾选图 4-35

中“要求安全通道(SSL)”复选框开启。客户端可以以 HTTPS 方式访问网站，而且可以下载服务器证书，验证证书合法性以及利用服务器证书公钥加密信息。若服务器和客户端要进行双向认证，亦即客户端验证服务器证书的合法性同时服务器也要验证客户端证书的合法性，以实现双向信任。要在客户端安装客户端证书而且在网站服务器图 4-35 界面上选中“要求客户端证书”单选按钮。

【问题 4】

本问题主要考查的是 HTTPS 的基本知识。

HTTPS 是基于安全目的的 HTTP 通道，其安全基础由 SSL 层来保证。最初由 netscape 公司研发，主要提供了通信双方的身份认证和加密通信方法。现在广泛应用于互联网上对安全敏感的通信，如网上交易、在线支付等。

安全套接层(Secure Sockets Layer, SSL)是一种安全协议，是网景公司(Netscape) 在推出 Web 浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL 在传输层对网络连接进行加密。

SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。它在服务器和客户机两端可同时被支持，目前已成为互联网上保密通信的工业标准。现行 Web 浏览器亦普遍将 HTTP 和 SSL 相结合，从而实现安全通信。此协议的继任者是 TLS。

IETF (www.ietf.org)将 SSL 作了标准化，即 RFC2246，并将其称为 TLS (Transport Layer Security)，其最新版本是 RFC5246，版本 1.2。从技术上讲，TLS1.0 与 SSL3.0 的差异非常微小。TLS 利用密钥算法在互联网上提供端点身份认证与通信保密，其基础是公钥基础设施(Public Key Infrastructure，PKI)。

【问题 5】

HTTPS 只是负责用户服务器和客户机交互时的合法性验证以及交互信息的安全，但不能保证服务器自身的安全，比如黑客攻击、DOS 攻击，这些防范是 HTTPS 做不到的。

4.2 DNS 服务器的配置

4.2.1 考点辅导

网络中的计算机必须知道目的计算机的 IP 地址才能与之通信，然而 Internet 上计算机的数量极为庞大，而且 IP 地址是一连串数字的组合，单从 IP 地址很难看出是哪一台计算机，也难以记忆，所以单纯让用户记住对方计算机的 IP 地址并以此来进行访问是不现实的。为了解决这个问题，可以为每台计算机指定一个唯一的、容易记忆的字符串名称，那么用户就可以直接通过计算机的名称来访问了。

随之而来的问题是，当用户使用目标计算机的名称访问对方时，自己的计算机仍需要知道目标计算机的 IP 地址，然后才能将其封装在数据包中通过网络发送给对方。然而用户并不知道目标计算机的 IP 地址，只知道其名称。为了解决这个矛盾，网络中必须有一种能够将计算机名称转换成其相应的 IP 地址，并将这个 IP 地址发送给用户所使用的计算机的服务。这样用户只需输入对方计算机的名称，而自己的计算机会自动通过这个服务获得该名称所对应的 IP 地址，从而实现计算机之间的通信，这就是所谓的“名称解析”。从上述的

过程可以看出，“名称解析”就是把目标计算机的名称转换为目标计算机 IP 地址的过程。目前，使用最为广泛的名称解析服务，就是域名系统(Domain Name System，DNS)。

DNS 是针对 ARPnet 的一些特殊问题发展而来的。早期的 ARPnet 只拥有几百台主机，只需要一个名为 hosts.txt 的文件就可以包含所有连接到 ARPnet 主机的名字-地址的映射。它通过将该文件定期更新并分发给各主机，来实现对整个网络主机信息的维护。但是随着网络规模的增长，这种方式开始无法满足要求，有时新的 hosts.txt 文件还没来得及分发到所有主机，一些主机的地址就已经改变，或是有新的主机添加到网络中。DNS 的产生，就是为了解决使用单一 hosts.txt 文件所带来的诸多问题。

计算机的名称主要有两种：完全合格域名(Full Qualified Domain Name，FQDN)和 NetBIOS 名。下面只介绍 Internet 上广泛使用的完全合格域名。

Internet 上的计算机数量众多，因此计算机的完全合格域名用的数量也十分庞大。为了便于对这些名称进行管理，必须按照某种方式把它们组织起来，以避免相互之间发生冲突。这种对计算机的完全合格域名进行组织的框架结构，称为“域名空间”。在“域名空间”中，为了便于对大量的计算机名称进行管理，引入了“域”的概念。所谓“域”，就是只包含了大量计算机名称的空间。例如，“com”就是一个域的名称，它代表了一个空间，里面包含了大量的计算机名称。

DNS 使用一种组织成层次结构的名字空间来为主机命名，确保了名字的唯一性，如图 4-36 所示。在域名空间中，最大域的名称为“.”，该域称为“根域”。Internet 上所有计算机的完全合格域名都被置于根域下，无一例外。为了进一步对根域中的计算机名称进行管理，在根域内分割了若干个子域，如 com、edu、net 和 gov 等，这些子域通常被称为“顶级域”。顶级域的完整域名由自己的域名与根域的名字组合而成，例如，“com”域的完整域名为“com.”。为了进一步对顶级域中的计算机名称进行管理，在顶级域内继续分割了若干个子域，这些子域称为“二级域”。例如，在“com.”下可以继续划分出 example、abc 等子域。二级域的完整域名由自己的域名和上一级域的域名组合而成，中间用“.”隔开。例如，二级域 example 的完整域名是 example.com.。以此类推，在二级域下还可以再分割出三级域等。在各个域中放置的计算机名称为“主机名”，主机名和其所在域的完整域名组成了这个主机的完全合格域名。例如，在图 4-36 中，主机 Host-A 的完全合格域名就是 Host-A.hello.example.com.。

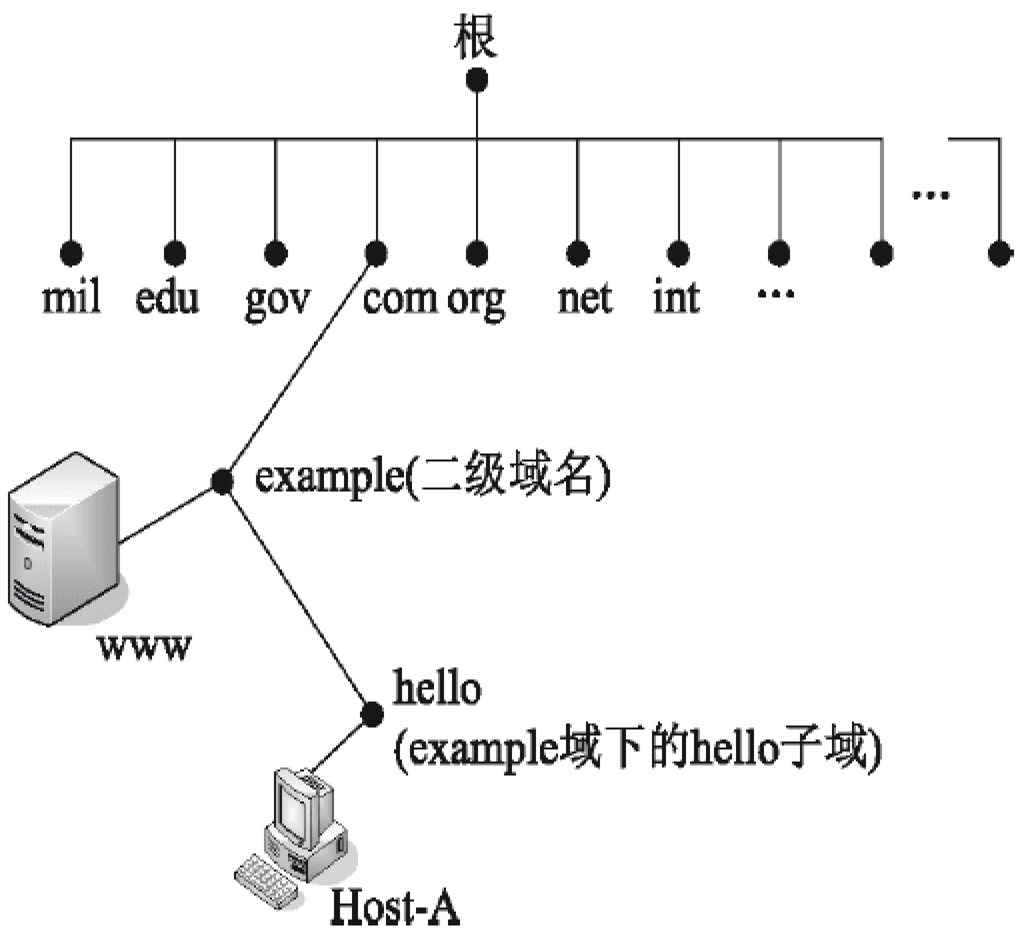


图 4-36 DNS 名字空间结构图

DNS 的这种结构类似于 Windows 中某个驱动器下的目录和文件结构。根域“.”对应于 Windows 中的“\”，各级域名的关系对应于目录和子目录，主机名对应于文件名。正是这种层次结构保证了名字的唯一性，就像一个目录下不可能有两个同名的文件一样。但在不同的域下，主机名是可以重复的。

在 Windows 中查看计算机的完全合格域名的方法为：右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，在打开的“系统属性”对话框中选择“计算机名”选项卡，在“完整的计算机名称”栏中显示的即为该计算机的完全合格域名，如图 4-37 所示。

图 4-37 “计算机名”选项卡

4.2.1.1 DNS 的工作原理

DNS 是 Internet 上非常重要的服务，因为现在人们在使用 Internet 时，几乎都在使用完全合格域名而非 IP 地址访问资源。可以说，人们在访问 Internet 资源的过程中始终需要 DNS 服务帮助将目标计算机名转换成 IP 地址，一旦 DNS 服务出现故障，将会导致 Internet 的瘫痪。

为了向用户提供完全合格域名的解析，需要在网络中安装和配置 DNS 服务器，并且将用户的计算机配置成某台或几台 DNS 服务器的客户机。DNS 客户机向 DNS 服务器提出查询请求，DNS 服务器对请求做出相应的应答。

DNS 查询以各种不同的方式进行解析。客户机有时可从以前查询获得的缓存中得到查询结果。DNS 服务器可以使用其自身缓存来应答查询，也可以通过查询或联系其他 DNS 服务器来解析客户机的查询，并将应答返回给客户机，这个过程称为递归。此外，客户机本身也可尝试联系其他 DNS 服务器来解析名称，这个过程称作迭代。

总之，DNS 查询过程按以下两部分进行。

(1) 查询传送至解析器进行解析，如果能在本地解析则返回结果。

(2) 如果不能在本地解析，则查询 DNS 服务器来解析名称。

下面详细解释这两个过程。

图 4-38 显示了完整的 DNS 查询过程。

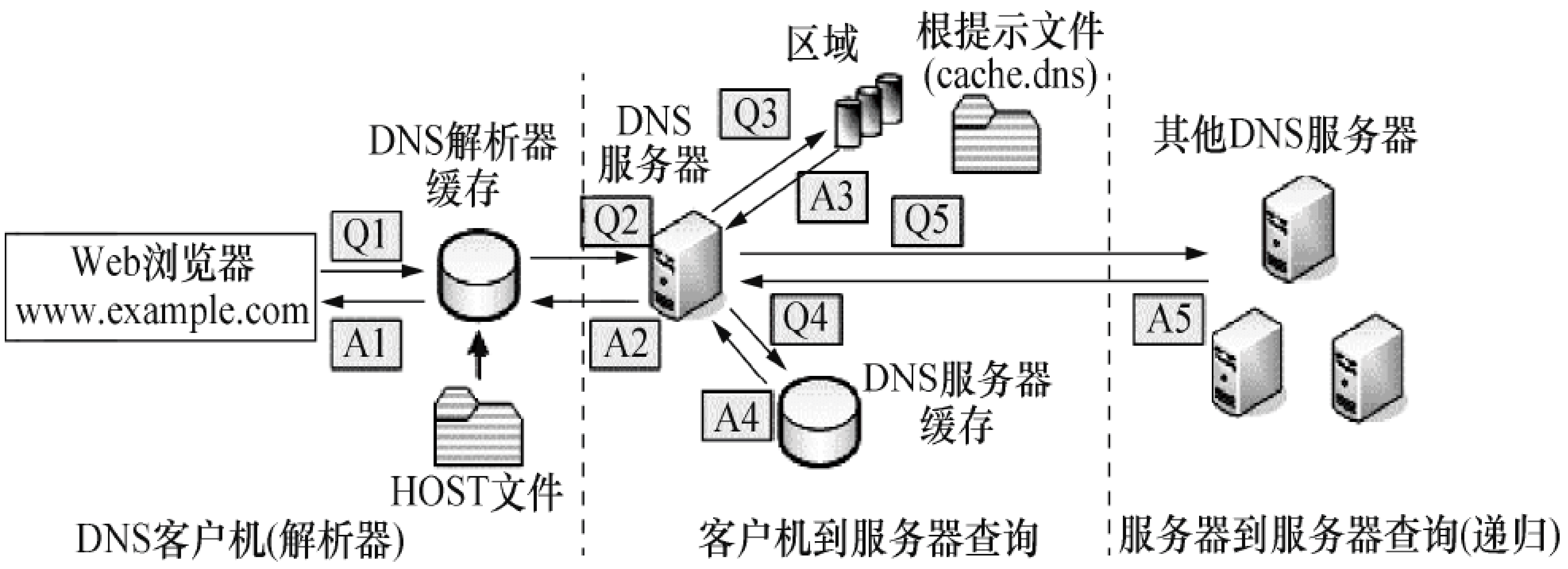


图 4-38　完整的 DNS 查询过程

本地解析的过程如图 4-38 所示中的 Q1 和 A1 两过程所示。假如用户在浏览器地址栏中输入 www.example.com，浏览器则会在与该地址所对应的主机通信前先向解析器查询该主机的 IP 地址。查询请求 Q1 传送至解析器，解析器检查本地缓存看能否进行就地解析。如果在缓存中找到相应的结果，则将结果发送给浏览器(A1)，本次查询结束。本地解析缓存中的名称信息可能有以下两个来源。

(1)　hosts 文件。如果该文件存在，则其中的任何主机名称到 IP 地址的映射在 DNS 客户服务启动时会预先加载到缓存中。

(2)　将在以前的 DNS 查询应答响应中获取的记录存储在本地 DNS 缓存中并保留一段时间。

如果在缓存中找不到匹配的信息，则解析过程继续进行，客户机将通过查询 DNS 服务器来解析名称。

如图 4-38 所示，客户机将查询主 DNS 服务器(Q2)。当 DNS 服务器收到查询时，首先检查它的本地配置区域中有没有与查询匹配的信息(Q3)。如果有，则服务器做出应答 A3，并且使用该信息来解析查询的名称(A2)。如果没有，服务器则检查它能否通过其缓存的先前查询信息来解析名称(Q4)。如果从中发现匹配的信息(A4)，服务器将向客户机返回该信息(A2)，查询完成。

如果通过上述步骤均未能找到匹配的信息，则查询过程继续进行。主 DNS 服务器将使用递归过程来从其他 DNS 服务器上获得信息，帮助其解析名称。在大多数情况下，DNS 服务器的默认配置支持递归过程，整个过程如图 4-39 所示。

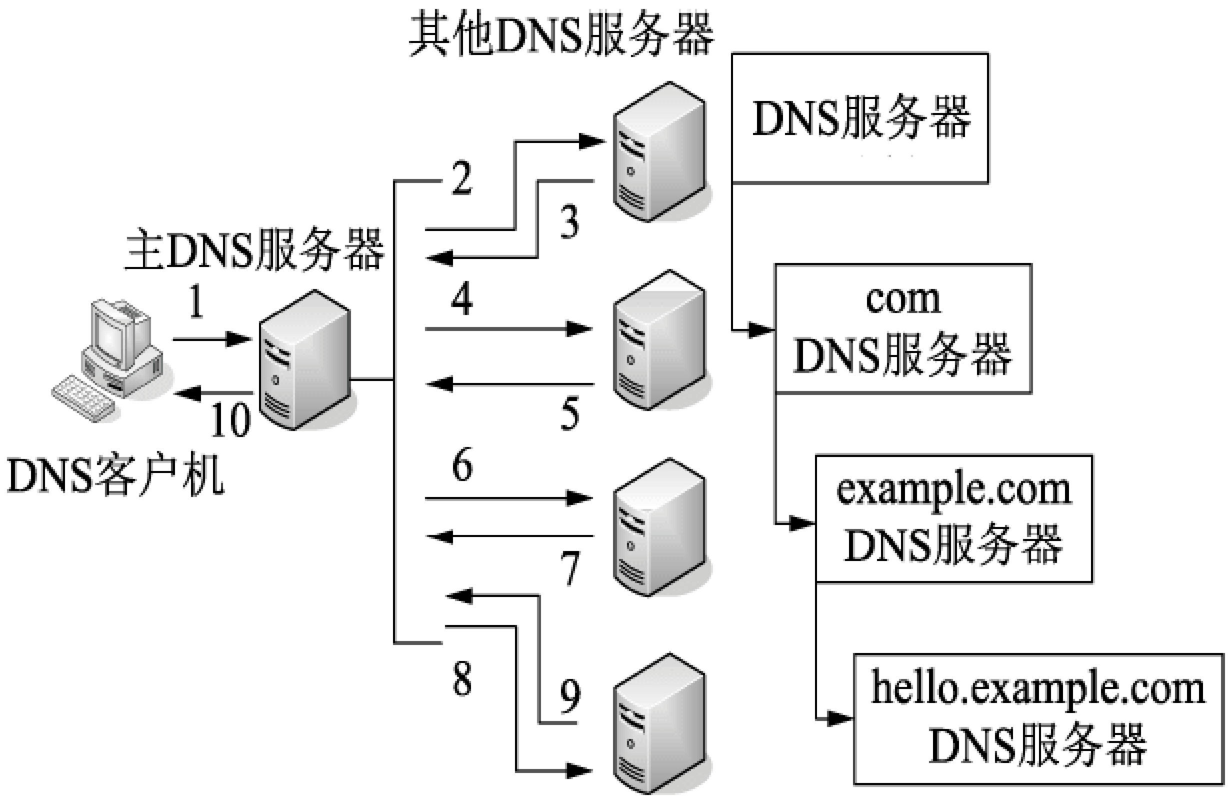


图 4-39　DNS 服务器的递归查询过程

如图 4-39 所示，假设客户机要查询的主机地址是 host.hello.example.com。首先，主服务器分析全名并确定对顶级域 com 具有绝对控制权的 DNS 服务器的 IP 地址。随后，对该服务器进行查询，以获取 example.com 子域 DNS 服务器的地址。接着再对 example.com 子域的 DNS 服务器进行查询，以获取 hello.example.comDNS 服务器的地址。最后，与 hello.example.com 子域的 DNS 服务器联系上。该服务器从其配置区域中查询到主机 host.hello.example.com 所对应的 IP 地址，并将结果返回给主 DNS 服务器，主服务器再将此应答转发给客户机，这样整个递归查询过程就完成了。

如果客户机使用迭代过程，则主 DNS 服务器就不需要像在递归方式下做那么多的工作，只需向客户机返回一个参考答复，其中包含有利于客户机解析请求的信息(如根提示信息等)，而不再进行其他操作；客户机根据 DNS 服务器返回的参考信息再决定处理方式。但是在实际网络环境中，禁用 DNS 服务器的递归查询往往会让 DNS 服务器对无法进行本地解析的客户端请求返回一个服务器失败的参考答复，此时，客户机则会认为解析失败。

递归方式和迭代方式的不同之处就是当 DNS 服务器没有在本地完成客户机的解析请求时，由谁扮演 DNS 客户机的角色向其他 DNS 服务器发起解析请求。通常情况下应使用递归方式，这样有利于网络管理和安全性控制。只是递归方式比迭代方式更消耗 DNS 服务器的性能，不过在通常的情况下，这点性能的消耗无关紧要。

4.2.1.2　安装 DNS 服务器和客户机

1. DNS 服务器的安装

Windows Server 2008 R2 系统内置了 DNS 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供域名解析服务。

在一台运行 Windows Server 2008 R2 的计算机上安装 DNS 服务器的操作步骤如下。

(1)　选择“开始”→“管理工具”→“服务器管理器”→“角色”命令，在打开的窗口中单击“添加角色”按钮，启动 Windows 添加角色向导。

(2)　在“服务器角色”列表框中勾选“DNS 服务器”复选框，并单击“下一步”按钮。按照向导提示，执行至确认界面，单击“安装”按钮，完成 DNS 服务器的安装。

2. 设置 DNS 服务器

安装完 DNS 服务器后，需要对其进行设置，这样 DNS 服务器才能为客户机提供服务。用于配置和管理 Windows Server 2008 R2 DNS 服务器的主要工具是 DNS 控制台 dnsmgmt。

从“管理工具”窗口中单击 DNS，可以看出 DNS 控制台已默认将本地服务器列在控制台左侧的树中。

假设局域网的域名为 example.com，其中有一台主机作为 WWW 服务器，IP 地址为 192.168.1.30，按照惯例将这台主机命名为 www.example.com。下面介绍如何在 DNS 服务器中实现对该主机名称的解析，步骤如下。

(1)　首先在 DNS 服务器中新建一个名为 example.com 的区域。右键单击控制台目录树中的 EX-WIN2008SVR 服务器，在弹出的快捷菜单中选择“配置 DNS 服务器”命令，打开“配置 DNS 服务器向导”对话框，单击“下一步”按钮。

(2)　在“选择配置操作”对话框中，为了讲解 DNS 服务器的配置，选择“创建正向和反向查找区域”，单击“下一步”按钮。

提示：正向查找区域用于进行 DNS 正向查询，即允许客户端通过已知的主机名，查找其所对应的 IP 地址；反向查找区域用于进行 DNS 反向查询，即允许客户端使用已知的 IP 地址，查找其所对应的计算机名。

(3) 在“新建区域向导”对话框中，由于此时配置的是网络内的第一台 DNS 服务器，所以选中“创建主要区域”单选按钮，单击“下一步”按钮。

(4) 在“区域名称”文本框中输入区域的名称 example.com，如图 4-40 所示，单击“下一步”按钮。

(5) 在“区域文件”向导页中，选中“创建新文件，文件名为”单选按钮，并使用系统默认的文件名 example.com.dns，单击“下一步”按钮，如图 4-41 所示。

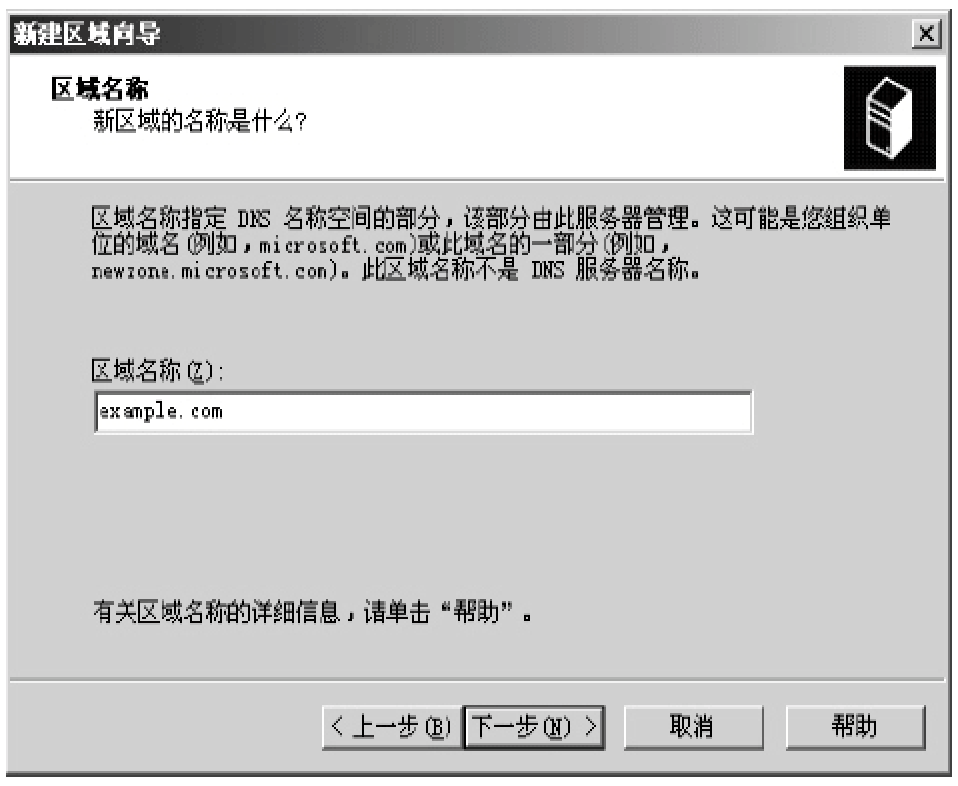


图 4-40　输入区域名称

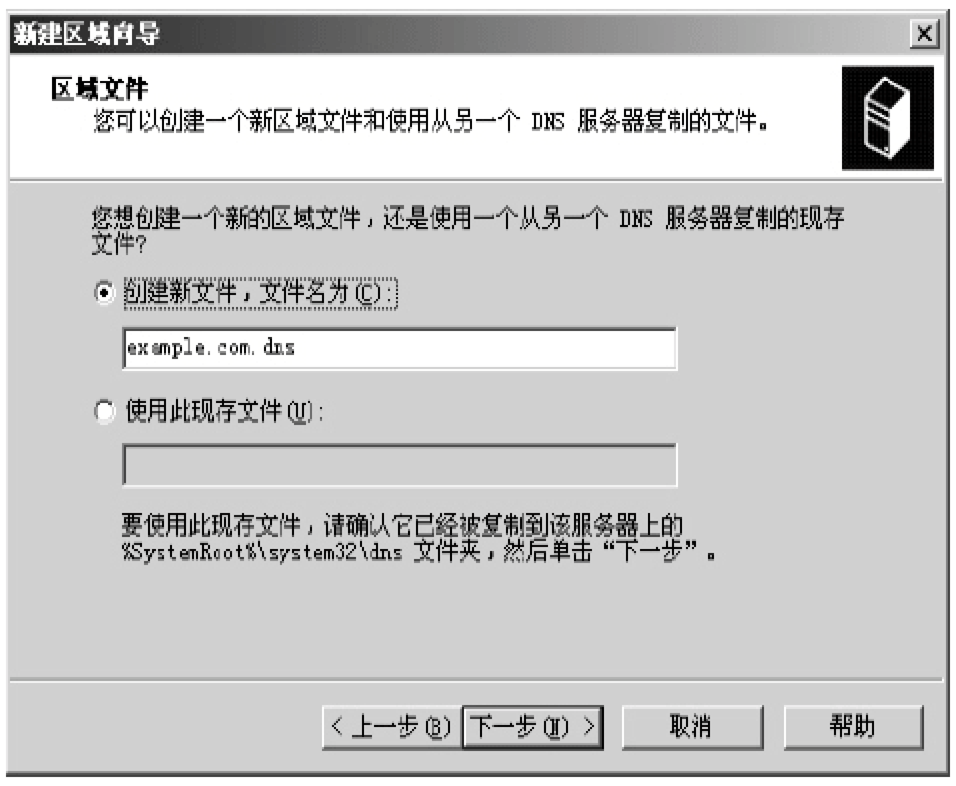
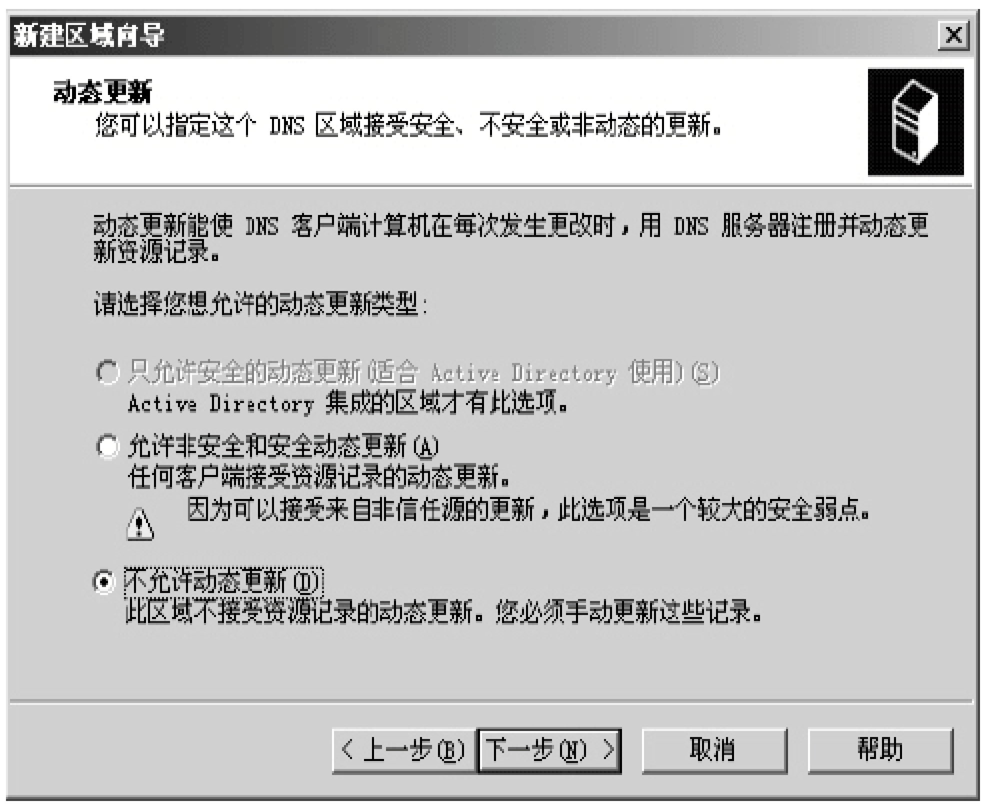


图 4-41　创建新的区域文件

(6) 在“动态更新”向导页中，选中“不允许动态更新”单选按钮，如果服务器已安装了 Active Directory，也可以选中“只允许安全的动态更新”单选按钮，以便最大限度地集成和支持 Active Directory 以及增强的 DNS 服务器功能。单击“下一步”按钮，如图 4-42 所示。

(7) 接下来配置反向区域，在“反向查找区域”向导页中，选中“是，现在创建反向查找区域”单选按钮，单击“下一步”按钮。在接下来的“区域类型”向导页中，依旧选中“主要区域”单选按钮，再单击“下一步”按钮。

(8) 在“反向查找区域名称”向导页中，选中“网络 ID”单选按钮，并在下面输入本网络的网络 ID，如 192.168.1，如图 4-43 所示，单击“下一步”按钮。



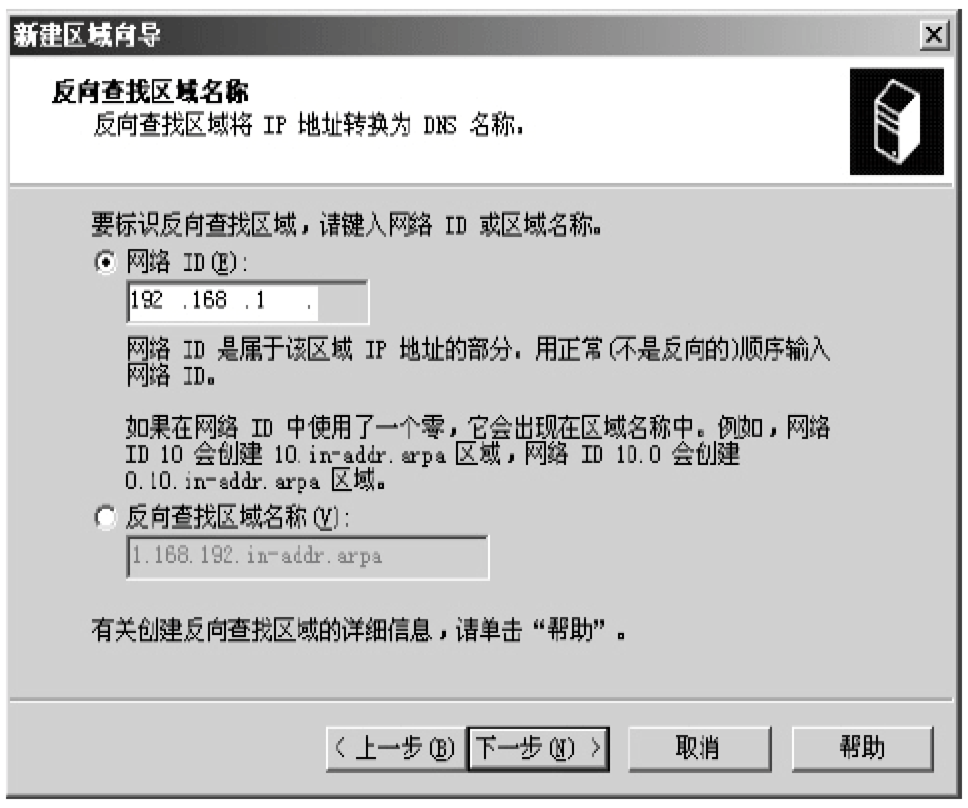


图 4-42　设置 DNS 服务器动态更新类型　　图 4-43　设置反向查找区域名称

(9) 在接下来的“区域文件”和“动态更新”两个页面中，分别选中“创建新文件，文件名为”和“不允许动态更新”单选按钮，文件名按照系统默认给出。

(10) 在“转发器”页面中，暂时选中“否，不向前转发查询”单选按钮。转发器的具体用途和配置方法后面会做进一步介绍。单击“下一步”按钮，如果配置顺利，会弹出一个对话框，提示已成功地完成了 DNS 服务器配置向导，单击“确定”按钮关闭对话框。

DNS 服务器配置完成后，在控制台的目录树中可以看到，服务器节点下建立了“正向查找区域”和“反向查找区域”。双击展开“正向查找区域”，会看到新区域 example.com 已经添加。单击 example.com，右半窗口中会显示该区域的配置信息。

3. 创建域名

下面介绍如何建立主机 www.example.com，其操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DNS 命令，打开 dnsmagt 控制台窗口。

(2) 在左窗格中依次展开 ServerName→“正向查找区域”目录，然后用鼠标右击区域名处，从弹出的快捷菜单中选择“新建主机”命令，弹出如图 4-44 所示的对话框，输入主机名 www，IP 地址 192.168.1.30。

(3) 如果希望 DNS 服务器也能够进行反向查询，则选中“创建相关的指针(PTR)记录”复选框，单击“添加主机”按钮。如果添加成功，系统会提示“成功地创建了主机记录 example.com。”，如图 4-45 所示，单击“确定”按钮。

图 4-44 “新建主机”对话框

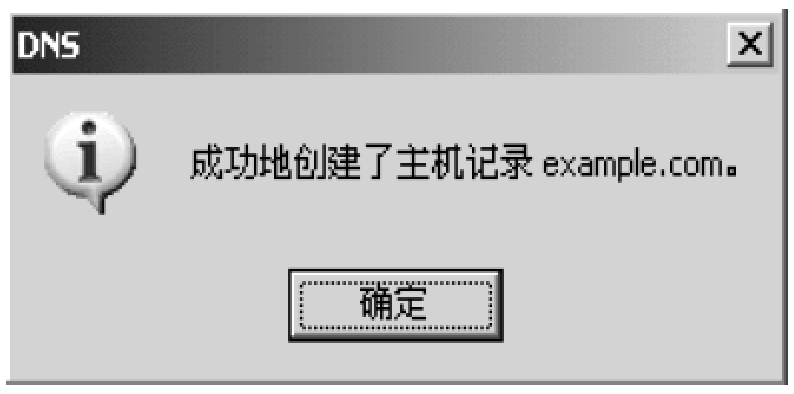


图 4-45 主机记录创建成功

(4) 如果不再添加主机，单击“完成”按钮。

4. 安装客户端

安装 DNS 客户机的步骤如下。

(1) 在“控制面板”对话框中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，在打开的“本地连接 属性”对话框中选中“Internet 协议(TCP/IP)”复选框，单击“属性”按钮，打开如

图 4-46 所示的对话框。

(4) 在图 4-46 的“首选 DNS 服务器”文本框中输入一台 DNS 服务器的 IP 地址，然后单击“确定”按钮，这样便把该计算机配置为那台 DNS 服务器的 DNS 客户机了。

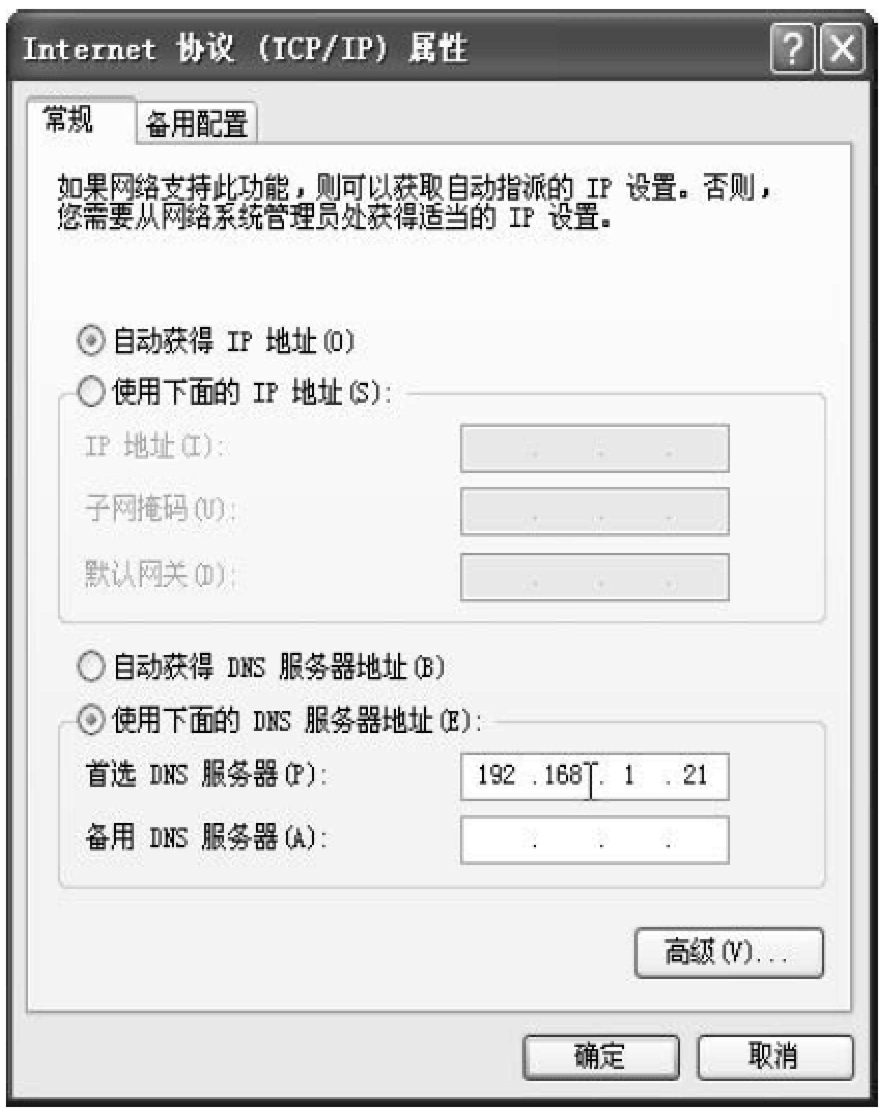


图 4-46　“Internet 协议(TCP/IP)属性”对话框

4.2.2　典型例题分析

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2017 年上半年下午试题三)

【说明】

请根据 Windows 服务器的安装与配置，回答下列问题。

【问题 1】(共 8 分)

图 4-47 是安装好的服务器管理器界面，在当前配置下，根域的名称是__(1)__。

图 4-47　“服务器管理器”界面

图示中角色服务配置时，建立域控制器 DC(Domain Controller)，需要通过命令行方式运行__(2)__命令；域中的 DC 和 DNS 配置在同一设备时，需要将独立服务器的首个 DNS 与 DC 的 IP 地址配置为__(3)__；DHCP 服务加入 DC 需要__(4)__，否则服务报错。

(2)备选答案：

A. dcomcnfg　　　　　　B. dcpromo

【问题 2】(共 6 分)

图 4-48 是 hosts 文件内容，图 4-49 是配置安全站点 https://webtest.com 的界面。

图 4-48　hosts 文件

图 4-49　配置安全站点

图 4-48 中，127.0.0.1webtest.com 的含义是__(5)__。在建立安全站点时，需要在 Web 服务器上启用__(6)__功能，并且绑定创建好的证书。

(6)备选答案：

A. SSL　　　　　　　　B. 代理

若将图 4-49 中 https 的端口号改为 8000，访问站点的 URL 是__(7)__。

【问题 3】(共 6 分)

图 4-50 是通过设备管理器查看到的信息，为安装驱动程序的设备提供__(8)__功能。

图 4-50　设备管理器

在“驱动程序”选项卡中会显示驱动程序提供商、驱动程序日期、驱动程序版本和__(9)__信息。

若更新驱动程序后无法正常运行，可以在该选项卡页面通过__(10)__操作将以前的驱动程序恢复。

(9)备选答案：

A. 数字签名　　　　B. 硬件类型

答案：

【问题 1】

(1) con-oso.com　(2) B　(3) 一样　(4) 授权

【问题 2】

(5) 在主机 hosts 表中建立 webtest.com 和 127.0.0.1 的对应关系　(6) A

(7) https://webtest.com:8000

【问题 3】

(8) 更新驱动程序　(9) A　(10) 回退驱动程序

解析：

【问题 1】con-oso.com 域林中第一个域树的名字就是根域的名字；dcomcnfig 命令用于开启“组件服务”配置；dcpromo 用于将服务器提升为域控制器，或者将域控制器降级为成员服务器，dcpromo 是 Windows 做域控制器的开关命令；根据题意，DNS 和 DC 的 IP 需要建立一种对应关系；加入 DC 控制域必须要授权。

【问题 2】访问 webtest.com，解析出 IP 为 127.0.0.1 相当于 DNS 的映射，当主机访问这个域名时会先到本机 host 文件找到这条记录解析成 127.0.0.1；安全站点 SSL 是 TCP 和应用层的安全协议通过数字证书加密建立安全站点绑定创建好的证书，SSL 可以对万维网客户与服务器之间传送的数据进行加密和鉴别。在双方握手阶段，对将要使用的加密算法和双方共享的会话密钥进行协商，完成客户与服务器之间的鉴别。在握手完成后，所传送的数据都使用会话密钥进行传输，以保证站点的安全性；默认的端口 443 是可以直接访问的，如果需要修改端口号访问，方法是域名后边加“:”端口号。

【问题 3】设备管理器是一种管理工具，可用它来管理计算机上的设备。可以使用“设备管理器”查看和更改设备属性、更新设备驱动程序、配置设备设置和卸载设备。在“驱动程序”选项卡中会显示驱动程序提供商、驱动程序日期、驱动程序版本和数字签名信息，打开窗口即可看到；通过回滚驱动程序，可以回到原来的驱动版本上。

4.2.3　同步练习

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】 网络拓扑结构如图 4-51 所示。

【问题 1】(4 分)

网络 A 的 WWW 服务器上建立了一个 Web 站点，对应的域名是 www.abc.edu。DNS 服务器 1 上安装了 Windows Server 2003 操作系统并启用 DNS 服务。为了解析 WWW 服务器的域名，在图 4-52 所示的对话框中，新建一个区域的名称是__(1)__；在图 4-53 所示的对话框中，添加的对应主机名称为__(2)__。

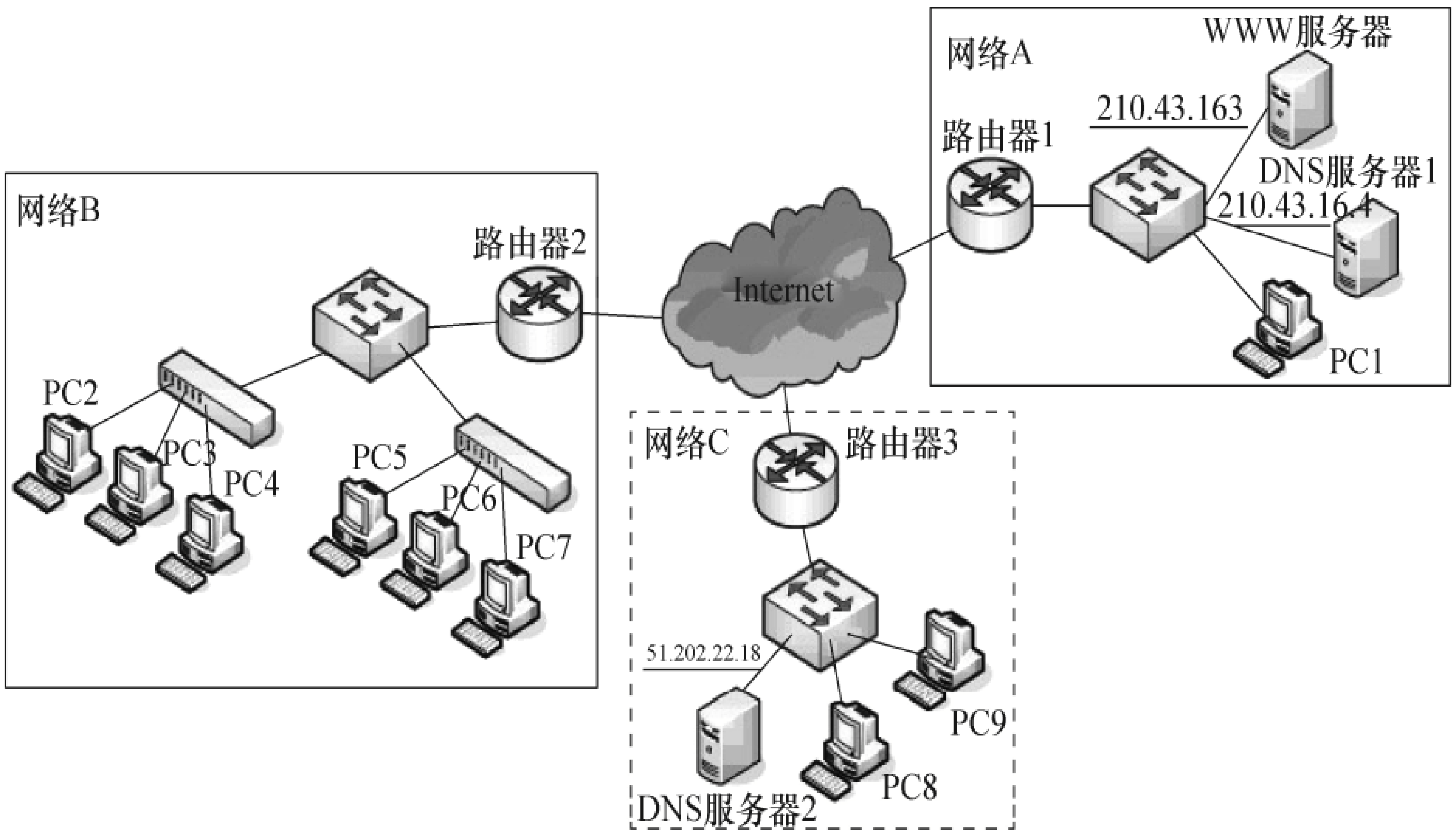


图 4-51　网络拓扑结构图

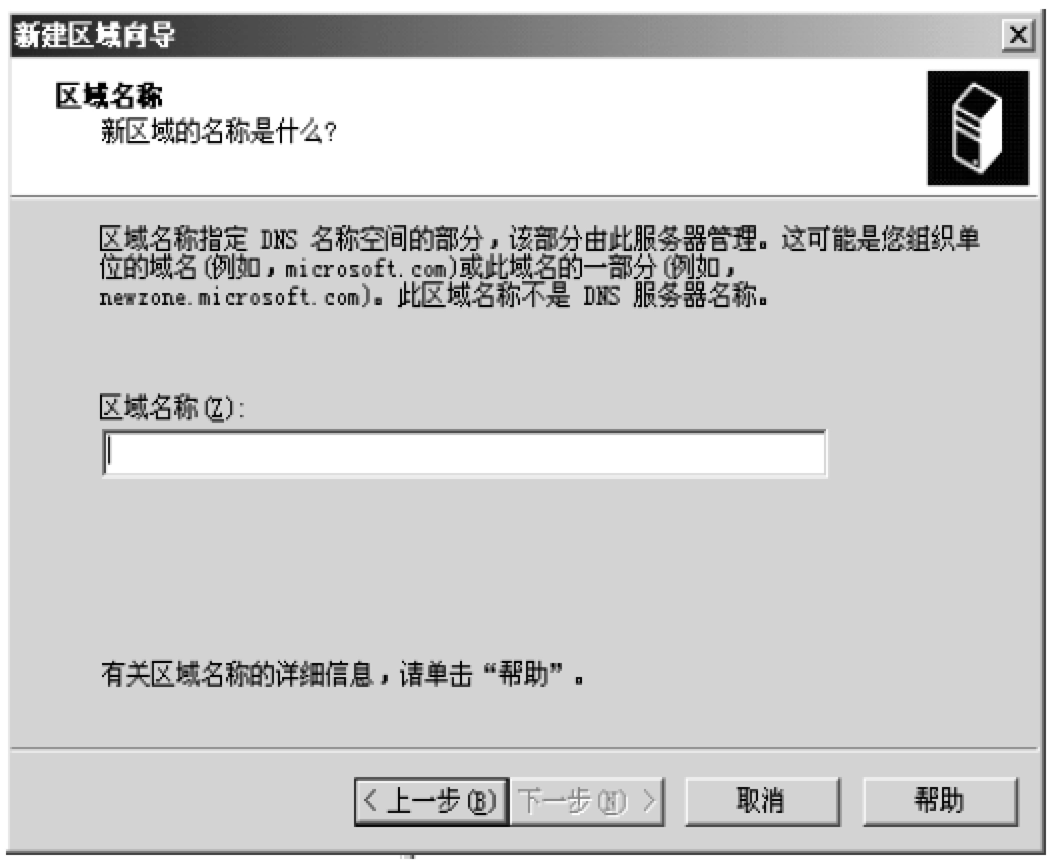


图 4-52　“新建区域向导”对话框

图 4-53　“新建主机”对话框

【问题 2】(3 分)

在 DNS 系统中反向查询(Reverse Query)的功能是__(3)__。为了实现网络 A 中 WWW 服务器的反向查询，在图 4-54 和图 4-55 中进行配置，其中网络 ID 应填写为__(4)__，主机名应填写为__(5)__。

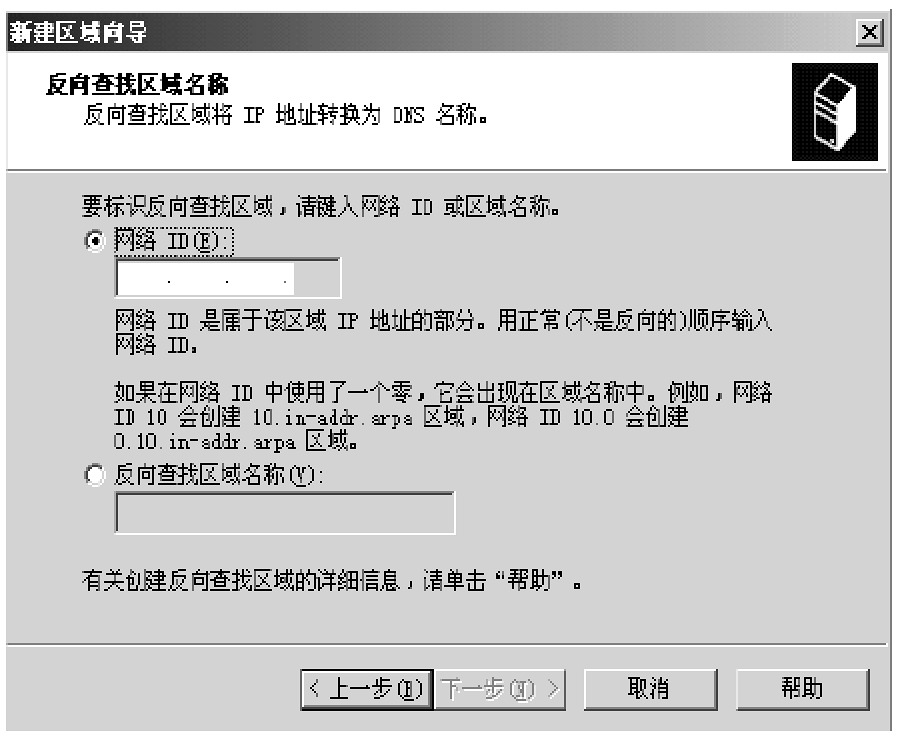


图 4-54　“反向查找区域名称”页面

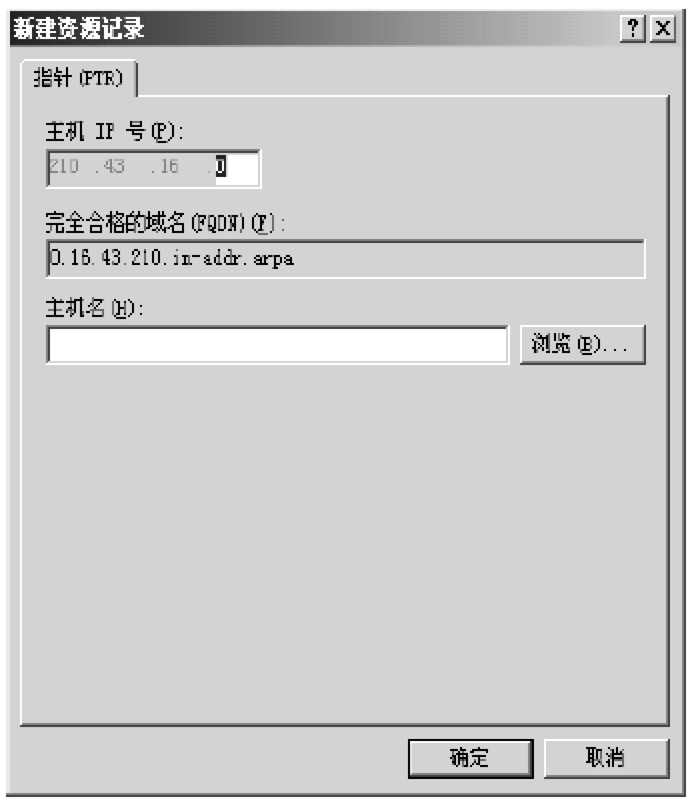


图 4-55　“新建资源记录”对话框

【问题 3】(3 分)

DNS 服务器 1 负责本网络区域的域名解析。对于非本网络的域名，可以通过设置“转发器”，将自己无法解析的名称转到网络 C 中的 DNS 服务器 2 进行解析。设置步骤：首先在“DNS 管理器”中选中 DNS 服务器，右击，选择“属性”对话框中的“转发器”选项卡，在弹出的如图 4-56 所示的对话框中应如何配置？

【问题 4】(2 分)

网络 C 的 Windows Server 2003 服务器上配置了 DNS 服务，在该服务器上两次使用 nslookup www.sohu.com 命令得到的结果如图 4-57 所示。由结果可知，该 DNS 服务器 <u>(6)</u> 。

(6) 备选答案：

A. 启用了循环功能　　B. 停用了循环功能

C. 停用了递归功能　　D. 启用了递归功能

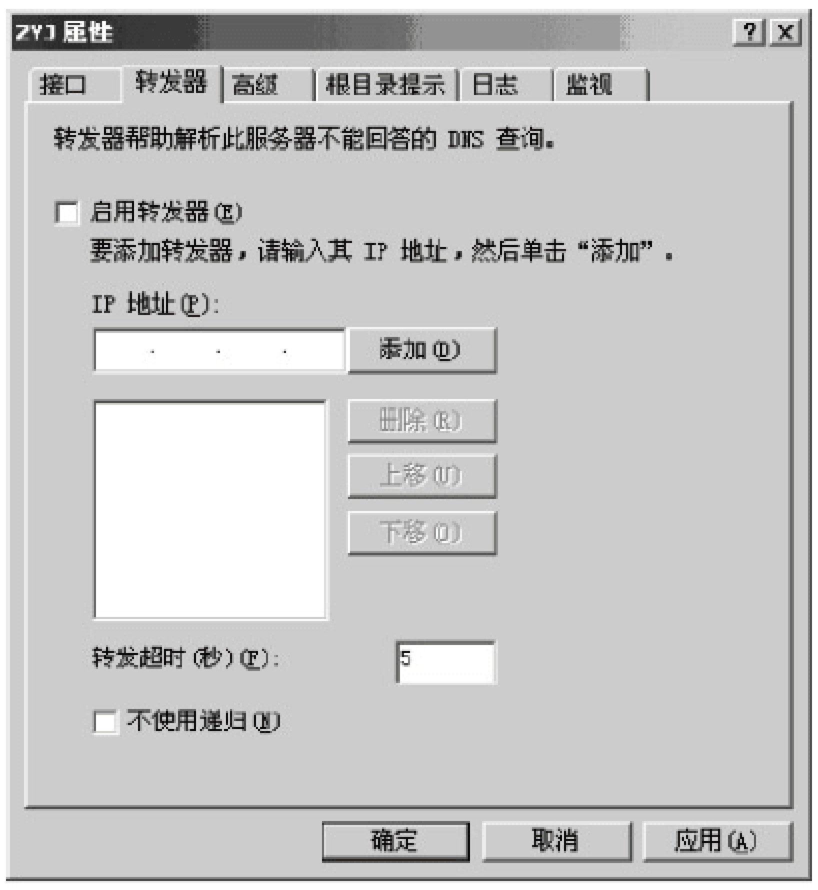
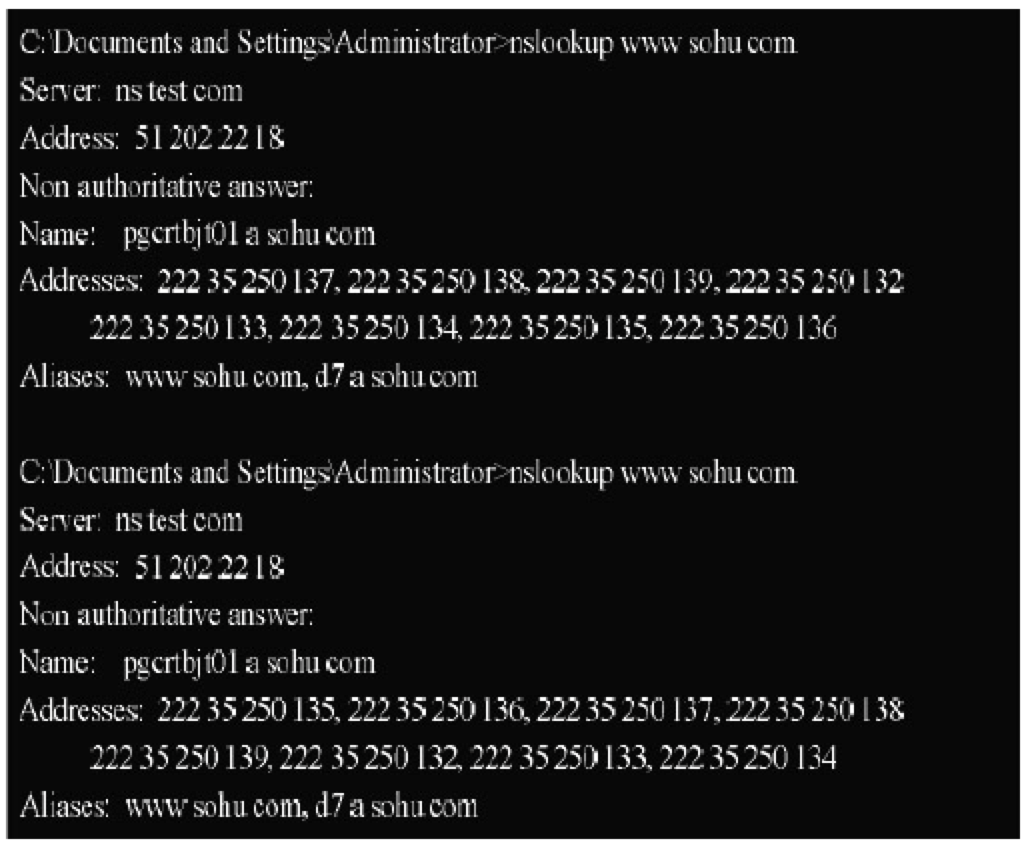


图 4-56　“转发器”选项卡



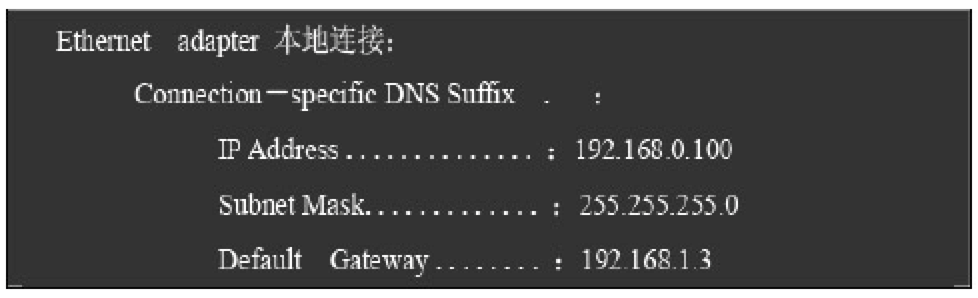
```
C:\Documents and Settings\Administrator>nslookup www sohu com
Server:  ns test com
Address:  51 202 22 18
Non authoritative answer:
Name:    pgcrtbjt01 a sohu com
Addresses:  222 35 250 137, 222 35 250 138, 222 35 250 139, 222 35 250 132
        222 35 250 133, 222 35 250 134, 222 35 250 135, 222 35 250 136
Aliases:  www sohu com, d7 a sohu com

C:\Documents and Settings\Administrator>nslookup www sohu com
Server:  ns test com
Address:  51 202 22 18
Non authoritative answer:
Name:    pgcrtbjt01 a sohu com
Addresses:  222 35 250 135, 222 35 250 136, 222 35 250 137, 222 35 250 138
        222 35 250 139, 222 35 250 132, 222 35 250 133, 222 35 250 134
Aliases:  www sohu com, d7 a sohu com
```

图 4-57　nslookup 命令执行结果

【问题 5】(3 分)

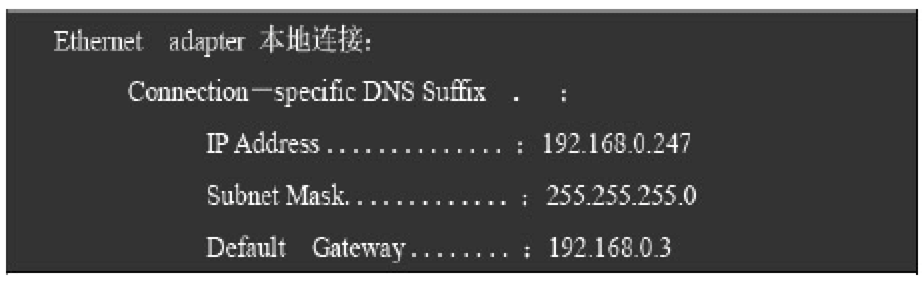
在网络 B 中，除 PC5 计算机以外，其他的计算机都能访问网络 A 的 WWW 服务器，而 PC5 计算机与网络 B 内部的其他 PC 都是连通的。分别在 PC5 和 PC6 上执行命令 ipconfig，结果信息如图 4-58 和图 4-59 所示。

请问 PC5 的故障原因是什么？如何解决？



```
Ethernet  adapter 本地连接:
      Connection—specific DNS Suffix  .   :
            IP Address . . . . . . . . . . . . . :  192.168.0.100
            Subnet Mask. . . . . . . . . . . . :  255.255.255.0
            Default   Gateway . . . . . . . . :  192.168.1.3
```

图 4-58　PC5 上 ipconfig 命令执行结果



```
Ethernet  adapter 本地连接:
      Connection—specific DNS Suffix  .   :
            IP Address . . . . . . . . . . . . . :  192.168.0.247
            Subnet Mask. . . . . . . . . . . . :  255.255.255.0
            Default   Gateway . . . . . . . . :  192.168.0.3
```

图 4-59　PC6 上 ipconfig 命令执行结果

4.2.4　同步练习参考答案

答案：

【问题 1】

(1) abc.edu　　(2) www

【问题 2】

(3) 通过 IP 地址查询域名　　(4) 210.43.16　　(5) www.abc.edu

【问题 3】

选中“启用转发器”复选框，在“IP 地址”文本框中输入“51.202.22.18”，单击“添加”按钮，然后单击“确定”按钮。

【问题 4】

(6) A

【问题 5】

PC5 的网关设置错误。重新设置 PC5 的网关，将其改为 192.168.0.3 即可。

4.3　DHCP 服务器的配置

4.3.1　考点辅导

4.3.1.1　DHCP 服务器的工作原理

动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)是一种 IP 标准，旨在通过使用运行有 DHCP 服务的服务器集中管理在网络上使用的 IP 地址和其他相关配置来降低系统管理员管理地址配置的复杂性。

前面介绍 TCP/IP 协议时，我们已经知道 TCP/IP 网络上的每台计算机都必须有一个唯一的计算机名和 IP 地址。如果在配置 IP 地址时不小心将同一 IP 地址分配给了网络中不同的计算机，系统会自动检测出该错误并提出警告。为了避免这种错误的产生，管理员在手工配置 IP 地址时必须记录每台计算机所对应的 IP 地址。这在小型的网络中还是可以接受的，但在拥有几百台甚至更多主机的网络中，管理员的工作会变得更加繁重，也更容易出错。此外，如果把一台主机从一个网络移到另一个网络，由于两个网络的地址配置方案可能不同，也要重新为该主机配置 IP 地址。当这种移动频繁发生时(如笔记本电脑)，使用静态 IP 地址分配方案同样会加大管理员的工作负担。而 DHCP 服务器能自动地为网络中的计算机分配 IP 地址，系统管理员只需在 DHCP 服务器上进行正确的配置，就可以完成整个网络地址的分配和配置。当网络中的某个配置参数改变时，管理员也只需在服务器端进行更改，新的配置就会应用到整个网络。

DHCP 也使用客户/服务器模式进行工作，通过配置，DHCP 服务器维护一个保存了 TCP/IP 配置信息的数据库来为客户机进行服务。DHCP 数据库中主要保存如下信息。

- 在地址池中维护可分配给客户机的 IP 地址以及用于手工指派的保留地址。
- 服务器提供的 IP 地址租约持续时间，租约时间指的是客户机从服务器获得 IP 地址后可以使用多长时间。
- 适用于所有客户机的其他配置选项，如可以为所有的客户机指定默认网关、DNS 服务器地址、WINS 服务器地址等多种选项。

DHCP 的工作过程如下。

1. DHCPDISCOVER

当 DHCP 客户机第一次登录网络时，会发现本机上没有设定任何的 TCP/IP 信息，它会向网络发出一个 DHCPDISCOVER 数据包。因为客户机还不知道自己属于哪一个网络，所以数据包的来源地址会为 0.0.0.0，而目的地址则为 255.255.255.255，然后再附上 DHCPDISCOVER 的信息，向网络进行广播，以便寻找能够为其分配 IP 地址的 DHCP 服务器。网络上每一台安装了 TCP/IP 协议的主机都会接收到这种广播信息，但只有 DHCP 服务器才会做出响应。

提示：DHCPDISCOVER 的等待时间预设为 1 秒，也就是当客户机将第一个 DHCPDISCOVER 数据包发送出去后，在 1 秒之内没有得到响应的话就会进行第二次 DHCPDISCOVER 广播。在得不到响应的情况下客户机一共会进行四次 DHCPDISCOVER 广播(包括第一次在内)。除了第一次会等待 1 秒之外，其余三次的等待时间分别是 9、13、16 秒。如果都没有得到 DHCP 服务器的响应，客户机则会显示错误信息宣告 DHCPDISCOVER 的失败，此时 Windows 会为自己临时分配一个位于 169.254.0.1～169.254.255.254 的 IP 地址(子网掩码为 255.255.0.0)。此后，系统仍会每隔 5 分钟再重新发送一次 DHCPDISCOVER 数据包，尝试与 DHCP 服务器联系。若联系成功，则使用由 DHCP 服务器提供的 TCP/IP 信息来更新自己的配置。

2. DHCPOFFER

当网络中的 DHCP 服务器收到客户机的 DHCPDISCOVER 数据包后，会在自己预先设定的可供分配的 IP 地址范围内选择一个尚未分配且最前面的 IP 地址，并连同其他 TCP/IP 设定，通过发送 DHCPOFFER 广播数据包，对 DHCP 客户机的请求做出响应。如果网络中有多台 DHCP 服务器，那么它们都会发送 DHCPOFFER 数据包对 DHCP 客户机做出响应，DHCP 客户机会从中选择其收到的第一个 DHCPOFFER 信息。

3. DHCPREQUEST

当 DHCP 客户机选择了第一个接收到的 DHCPOFFER 数据包后，将发送一个 DHCPREQUEST 广播数据包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。之所以要以广播方式回答，是为了通知所有的 DHCP 服务器，它将选择某台 DHCP 服务器所提供的 IP 地址。同时，客户机还会向网络发送一个 ARP 数据包，查询网络上面有没有其他机器使用该 IP 地址；如果发现该 IP 已经被占用，客户机则会发出一个 DHCPDECLINE 数据包给 DHCP 服务器，拒绝接受其 DHCPOFFER，并重新发送 DHCPDISCOVER 信息。

4. DHCPACK

当 DHCP 服务器收到 DHCP 客户机回答的 DHCPREQUEST 请求信息之后，便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置(子网掩码、默认网关、DNS 服务器地址等)的 DHCPACK 确认信息，告诉 DHCP 客户机可以使用它所提供的 IP 地址。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定。另外，除 DHCP 客户机选中的服务器外，其他的 DHCP 服务器都将收回曾提供的 IP 地址。

DHCP 客户机获得的 IP 地址是有使用期限的，这个使用期限由提供 IP 地址的 DHCP

服务器设定。默认情况下，在 Windows Server 2003 中，这个期限为 8 天。为了延长 IP 地址的使用期限，DHCP 客户机需要更新 IP 地址租约。更新的方法有两种：自动更新和手工更新。

1) 自动更新

在以下几种情况下，DHCP 客户机会自动向 DHCP 服务器更新 IP 地址租约。

- 当 DHCP 客户机租用的 IP 地址期限过一半时，客户机会自动向为其提供 IP 地址的 DHCP 服务器发送 DHCPREQUEST 广播数据包，以便要求继续租用原来的 IP 地址。如果续租成功，则新租约代替原租约；如果续租失败，则继续使用原来的 IP 地址。
- 如果 IP 地址租约期限过一半时，续租没有成功，则在剩下的租约期限再过一半的时候，DHCP 客户机会自动发送 DHCPDISCOVER 广播数据包，向网络中的任何一台 DHCP 服务器请求获得一个新的 IP 地址租约。
- 每当 DHCP 客户机重新启动时，也会自动向为其提供 IP 地址的 DHCP 服务器发送 DHCPREQUEST 广播数据包，要求继续租用 IP 地址。

2) 手工更新

用户可在 DHCP 客户机上使用 ipconfig /renew 命令手工对 IP 地址租约进行更新，另外也可以随时释放已有的 IP 地址租约，操作命令为 ipconfig /release。

4.3.1.2 安装 DHCP 服务器和客户机

1. 安装 DHCP 服务器

Windows Server 2008 R2 系统内置了 DHCP 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供 DHCP 服务。将一台运行 Windows Server 2008 R2 的计算机配置成 DHCP 服务器，最简单的方法是使用服务器管理器添加 DHCP 服务器角色，其过程如下。

(1) 通过“开始”菜单打开“服务器管理器”窗口，选择左侧的“角色”节点，单击“添加角色”超链接，启动添加角色向导。

(2) “开始之前”向导页中提示了此向导可以完成的工作，以及操作之前应注意的相关事项，单击“下一步”按钮继续。

(3) “选择服务器角色”向导页中显示了所有可以安装的服务器角色。如果角色前面的复选框没有被选中，则表示该网络服务尚未安装。如果已选中，则说明该服务已经安装。这里选中“DHCP 服务器”复选框，单击“下一步”按钮继续。

(4) “DHCP 服务器”向导页中对 DHCP 服务器的功能作了简要介绍，单击“下一步”按钮继续。

(5) 在“选择网络连接绑定”向导页中选择此 DHCP 服务器将用于向客户端提供服务的网络连接，单击“下一步”按钮继续，如图 4-60 所示。

(6) 在“指定 IPv4 DNS 服务器设置”向导页中指定客户用于名称解析的父域名，以及客户端用于域名解析的 DNS 服务器 IP 地址，单击“下一步”按钮继续，如图 4-61 所示。

(7) 在“指定 IPv4 WINS 服务器设置”向导页中选择是否使用 WINS 服务，单击“下一步”按钮继续，如图 4-62 所示。

(8) 在“添加或编辑 DHCP 作用域”向导页中可以添加 DHCP 作用域。只有指定了作

用域，DHCP 服务器才能向客户端分配 IP 地址、子网掩码和默认网关等。现在可以不指定，等 DHCP 安装完成后再添加。若现在指定，可单击“添加”按钮，如图 4-63 所示。

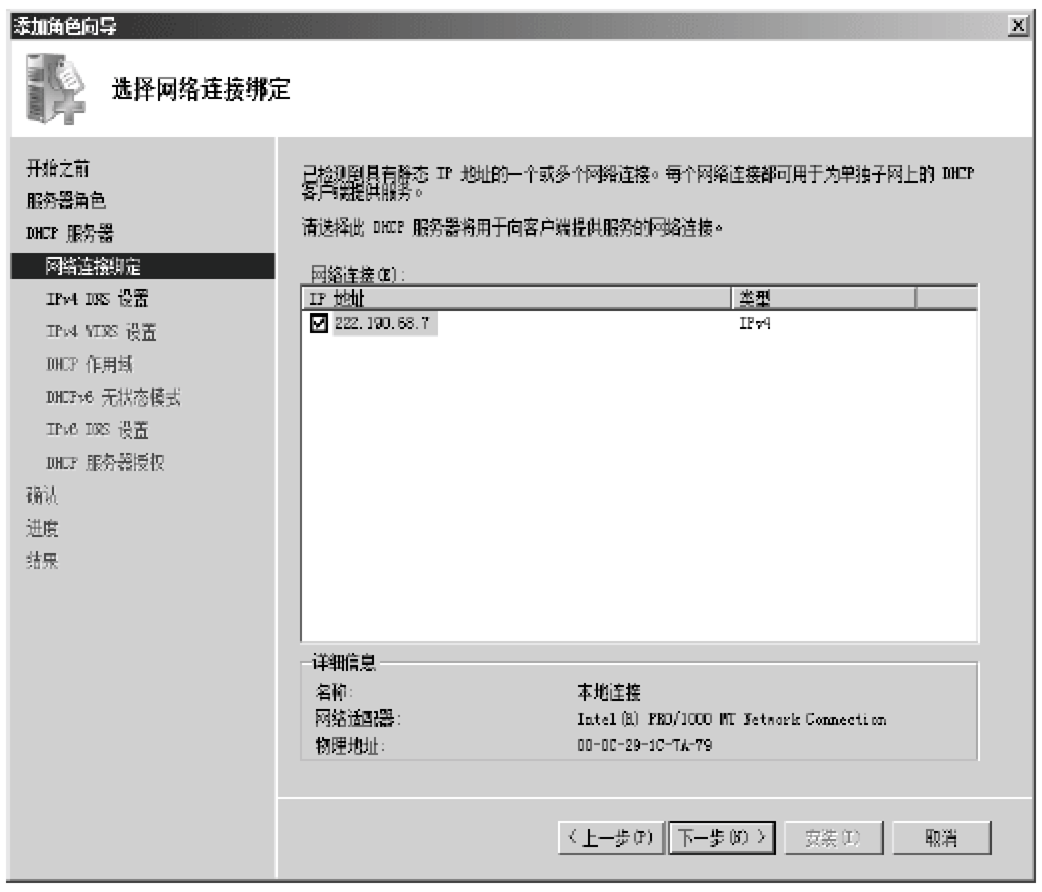


图 4-60　选择网络连接绑定

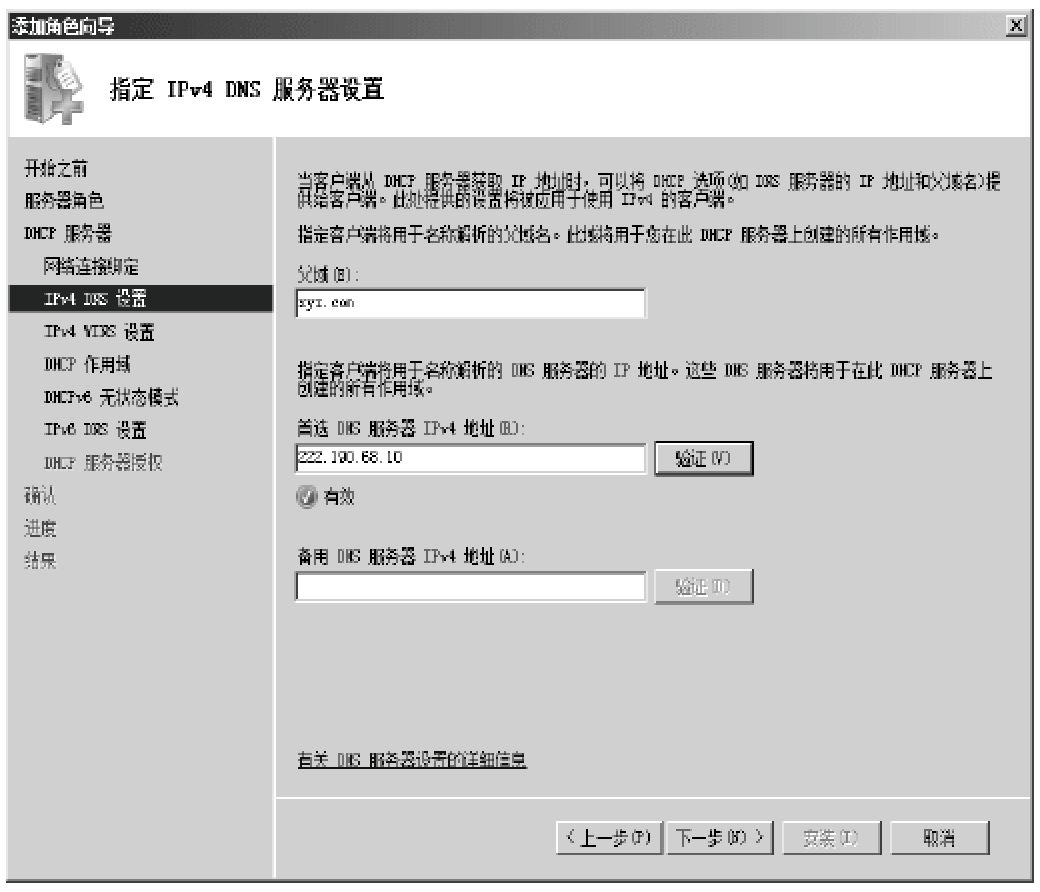


图 4-61　指定 IPv4 DNS 服务器设置

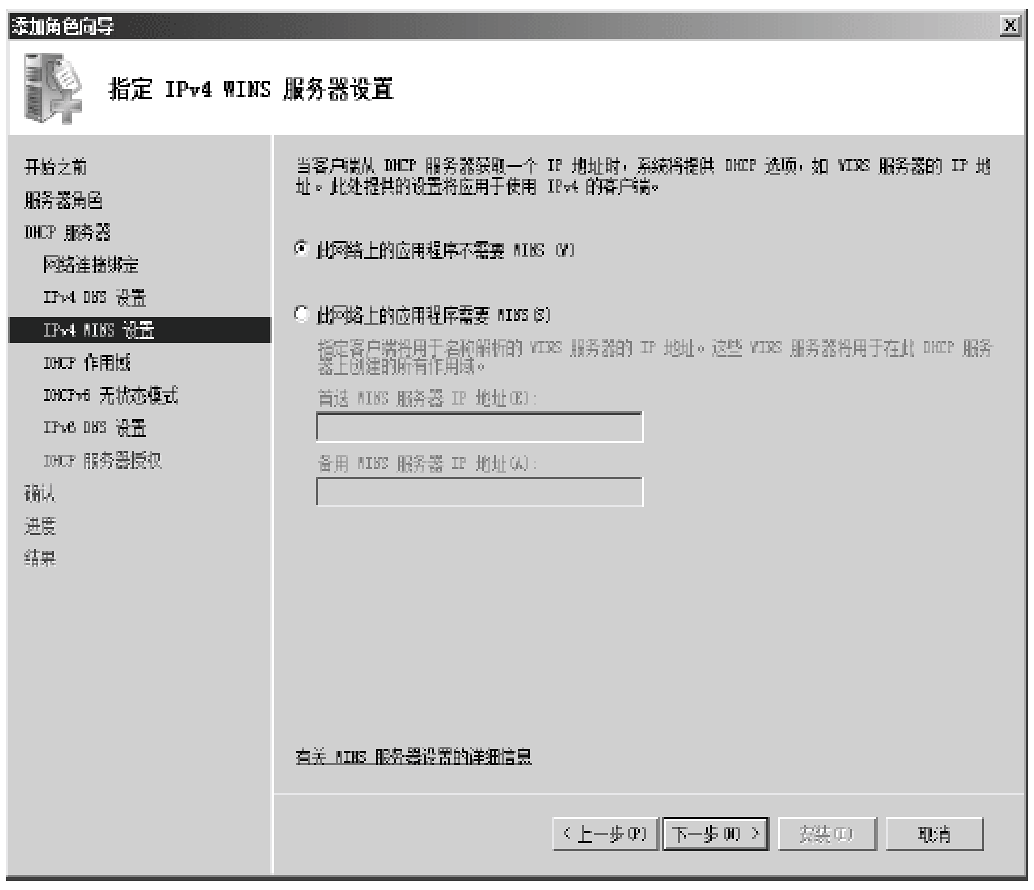


图 4-62　指定 IPv4 WINS 服务器设置

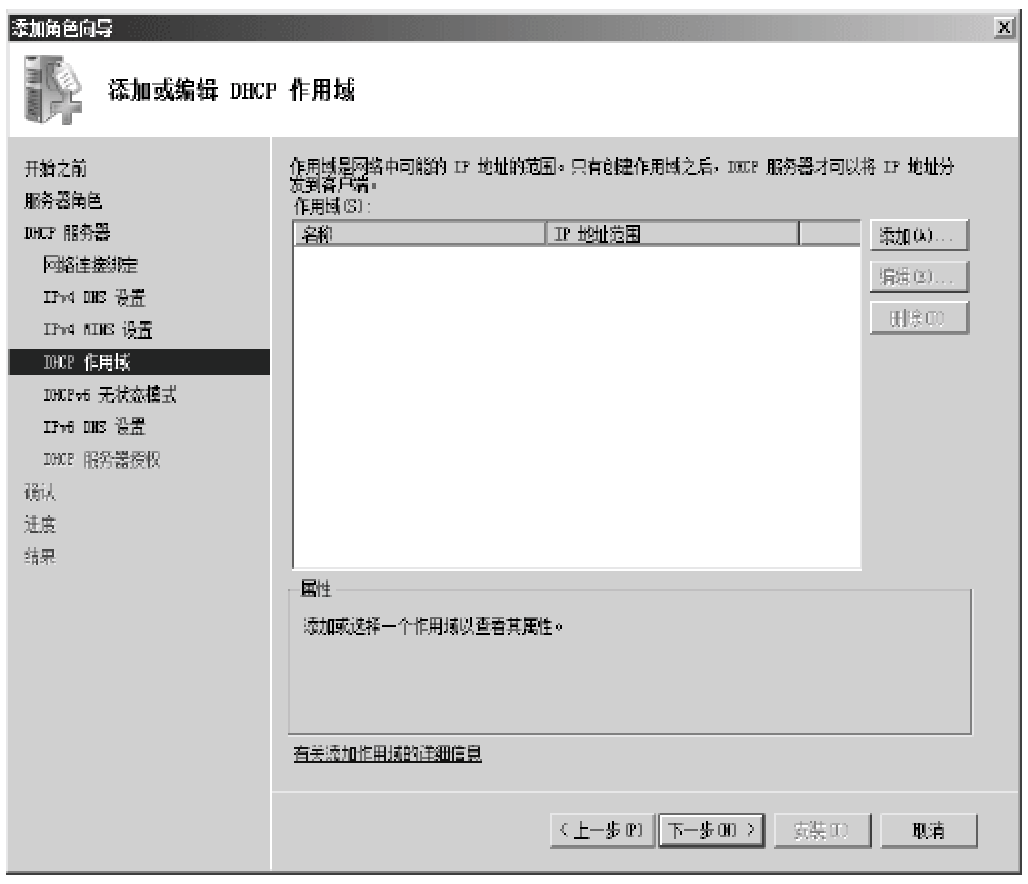


图 4-63　添加或编辑 DHCP 作用域

(9)　在“添加作用域”对话框中设置作用域的名称、起始 IP 地址、结束 IP 地址、子网掩码、默认网关以及子网类型。若选中“激活此作用域”复选框，则创建完成后会自动激活，如图 4-64 所示。设置完成后，单击“确定”按钮，返回上一步操作后单击“下一步”按钮继续。

(10) 在“配置 DHCPv6 无状态模式”向导页中选择启用还是禁用服务器的 DHCPv6 无状态模式。选中“对此服务器禁用 DHCPv6 无状态模式”单选按钮，单击“下一步”按钮继续，如图 4-65 所示。

(11) 若 DHCP 服务器已加入了域，还会打开“授权 DHCP 服务器”向导页，若没有加入域，则不会出现此向导页。为 DHCP 服务器授权必须具有域管理员的权限，若当前没有以域管理员身份登录到域，则选中“使用备用凭据”单选按钮，然后单击“指定”按钮输入域管理员的用户名及密码。单击“下一步”按钮继续，如图 4-66 所示。

(12) 在“确认安装选择”向导页中，要求确认所要安装的服务器角色及配置情况，如果配置错误，可以单击“上一步”按钮返回。单击“安装”按钮即可开始安装 DHCP 服务器角色，如图 4-67 所示。

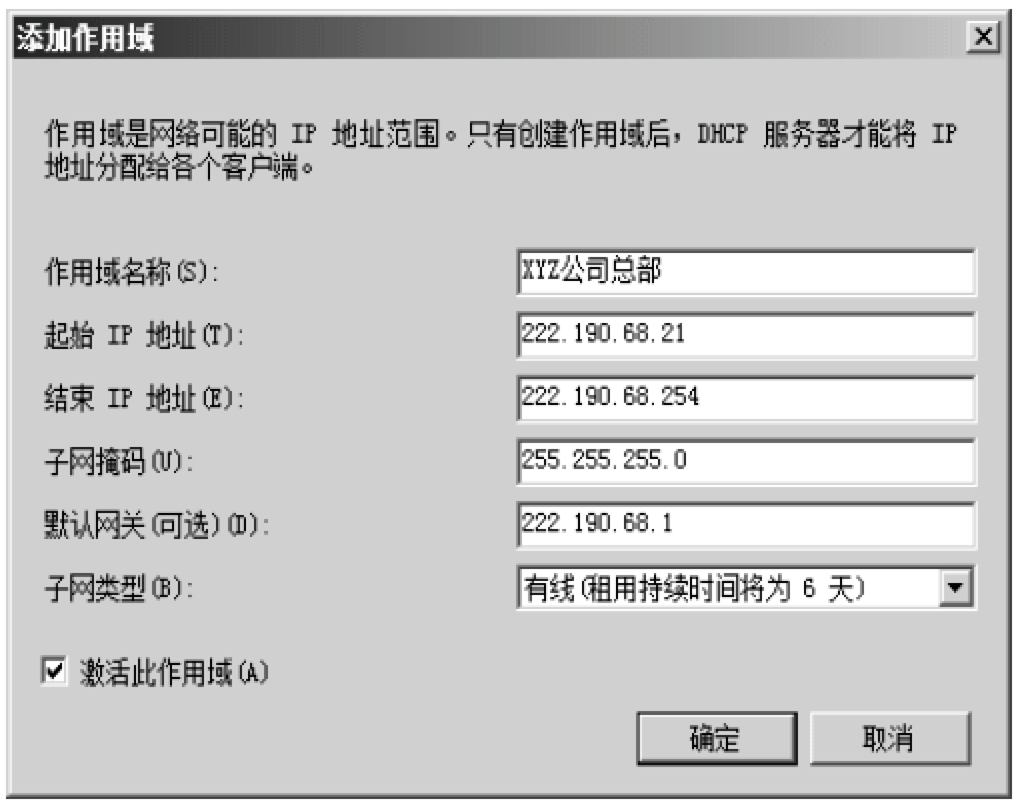


图 4-64　添加作用域

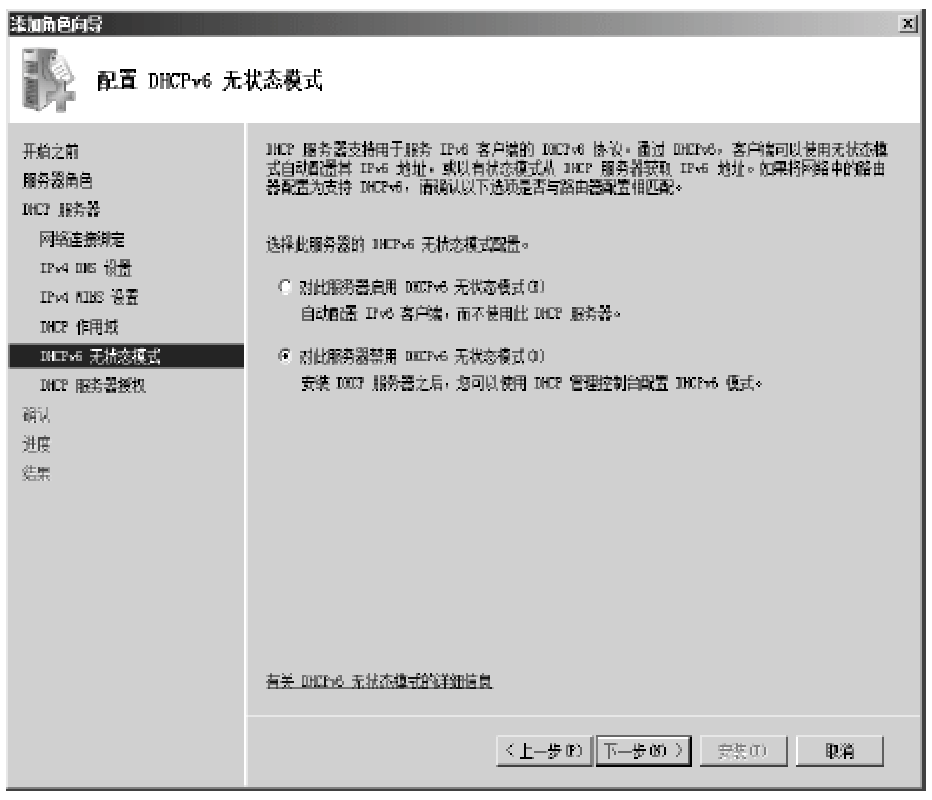


图 4-65　配置 DHCPv6 无状态模式

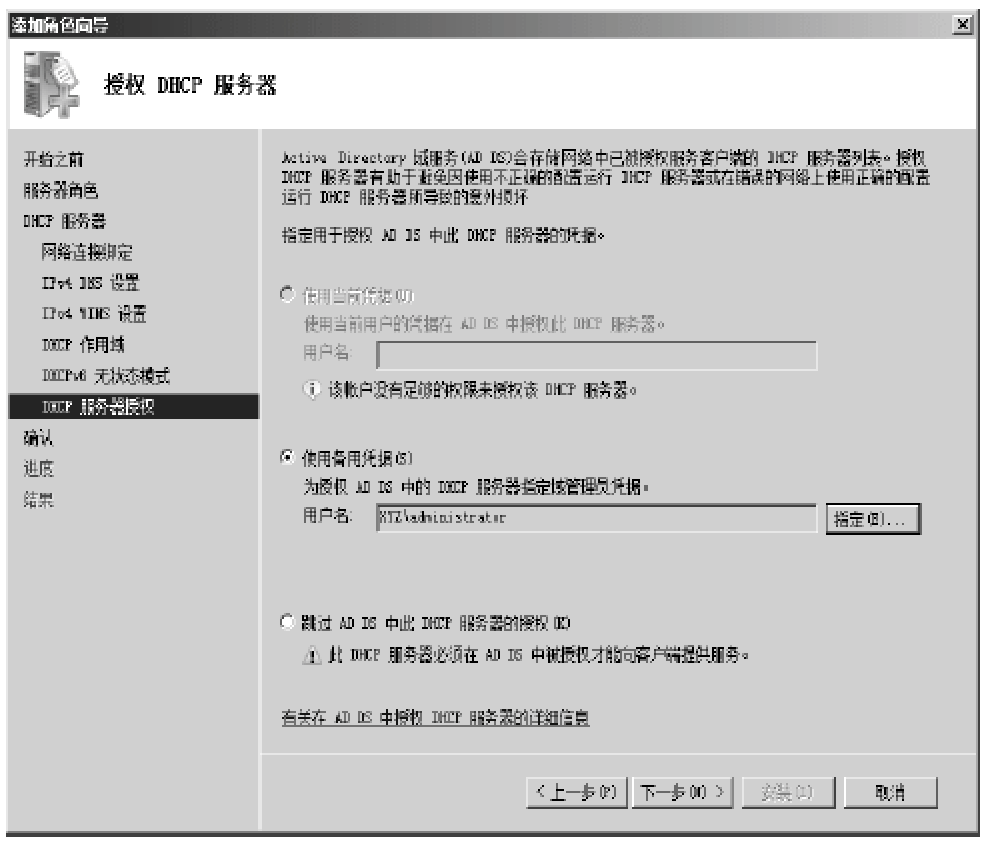


图 4-66　授权 DHCP 服务器

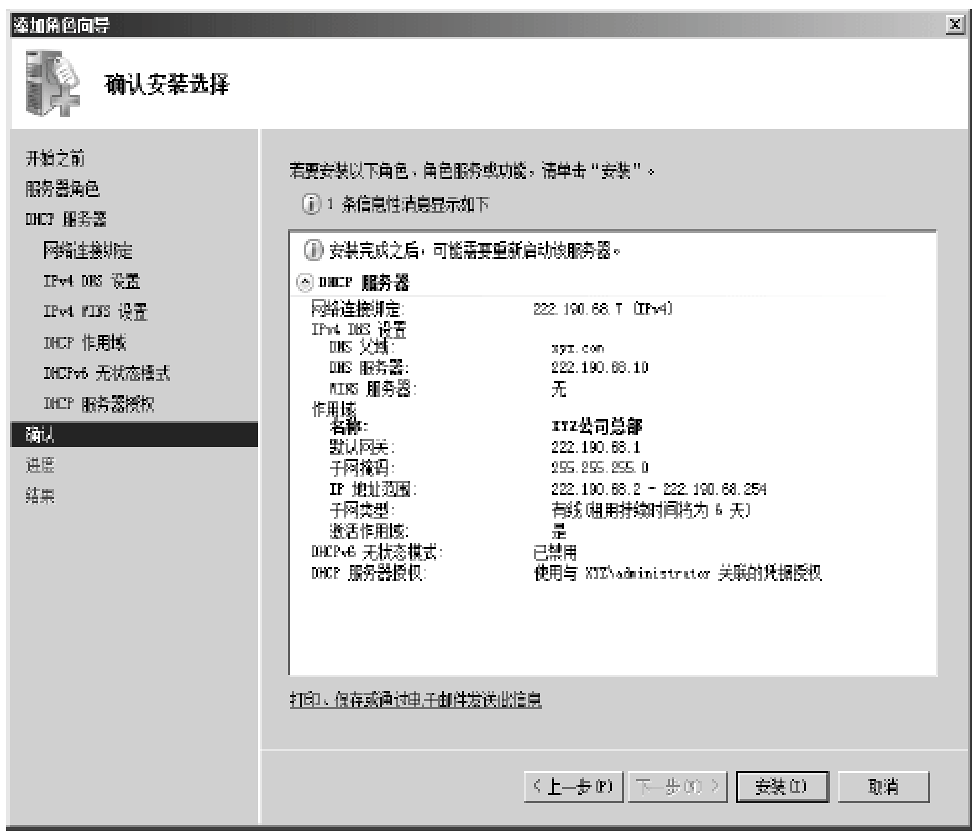


图 4-67　确认安装选择

(13) “安装进度”向导页中显示了安装 DHCP 服务器角色的进度，需耐心等待。

(14) “安装结果”向导页中显示 DHCP 服务器角色已经安装完成，提示用户可以使用 DHCP 管理器对 DHCP 服务器进行配置。若系统未启用 Windows 自动更新，还提醒用户设置 Windows 自动更新，以即时给系统打上补丁。单击“完成”按钮关闭添加角色向导便完成了 DHCP 服务器的安装。

DHCP 服务器安装完毕后，可以通过选择“开始”→“管理工具”→DHCP 命令打开 DHCP 管理器，通过 DHCP 窗口可以管理本地或远程的 DHCP 服务器，如图 4-68 所示。

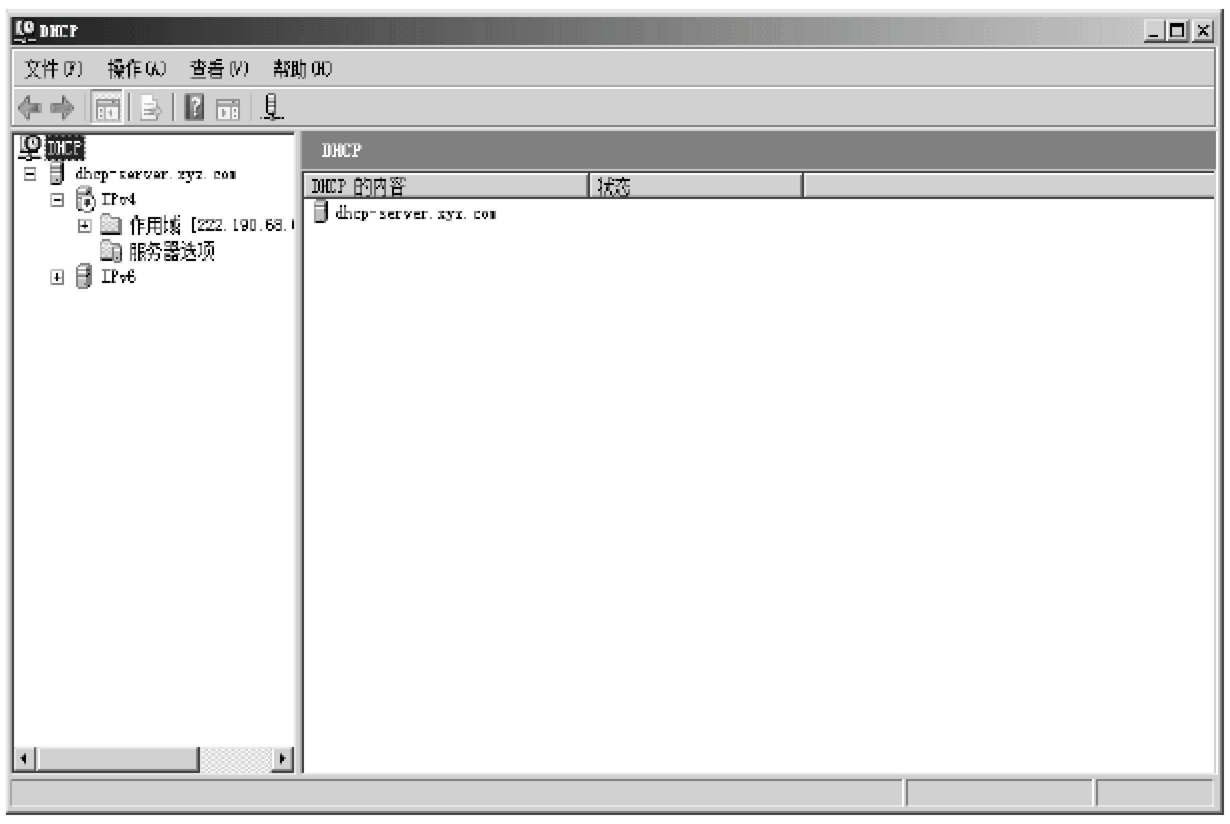


图 4-68　DHCP 管理器

2. 安装 DHCP 客户机

如果希望某台计算机能够自动获取 IP 地址，则需将这台计算机配置为 DHCP 客户机，配置方法如下。

(1) 在“控制面板”中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右键单击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，选中“Internet 协议(TCP/IP)”，单击“属性”按钮，打开“Internet 协议(TCP/IP)属性”对话框。

(4) 选中“自动获得 IP 地址”单选按钮，然后单击“确定”按钮，这样便把该计算机配置为 DHCP 客户机了。

4.3.1.3　设置 DHCP 服务器

在安装了 DHCP 服务器之后，还需要在 DHCP 服务器上建立一个或多个 IP 地址作用域。“IP 地址作用域”是指可以分配给 DHCP 客户机的 IP 地址范围。这样，当 DHCP 客户机向 DHCP 服务器请求 IP 地址时，DHCP 服务器就可以从 IP 地址作用域中选择一个尚未被租用的 IP 地址，将其分配给 DHCP 客户机。

新建作用域的操作步骤如下。

(1) 依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。

(2) 在左侧窗格中，右键单击服务器名，在弹出的快捷菜单中选择“新建作用域”命令。

(3) 在弹出的“新建作用域向导”对话框中单击“下一步”按钮。

(4) 在“名称”文本框中输入一个能够清楚表示该作用域的名称，如图 4-69 所示。

(5) 单击“下一步”按钮，打开设置“IP 地址范围”的向导页。地址范围通过设置“起始 IP 地址”和“结束 IP 地址”来指定。通过设置“长度”，用户可以调整子网掩码，以指定 IP 地址中多少位作为网络 ID，多少位作为主机 ID，如图 4-70 所示。

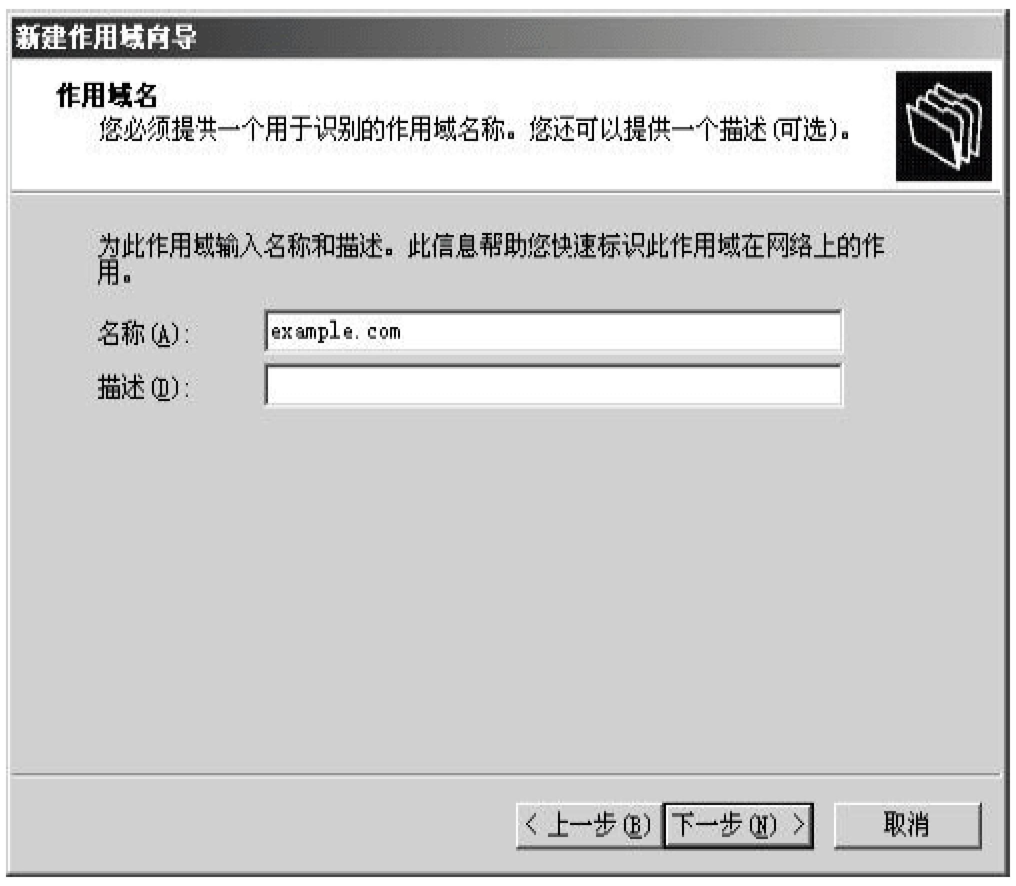


图 4-69　设置作用域名

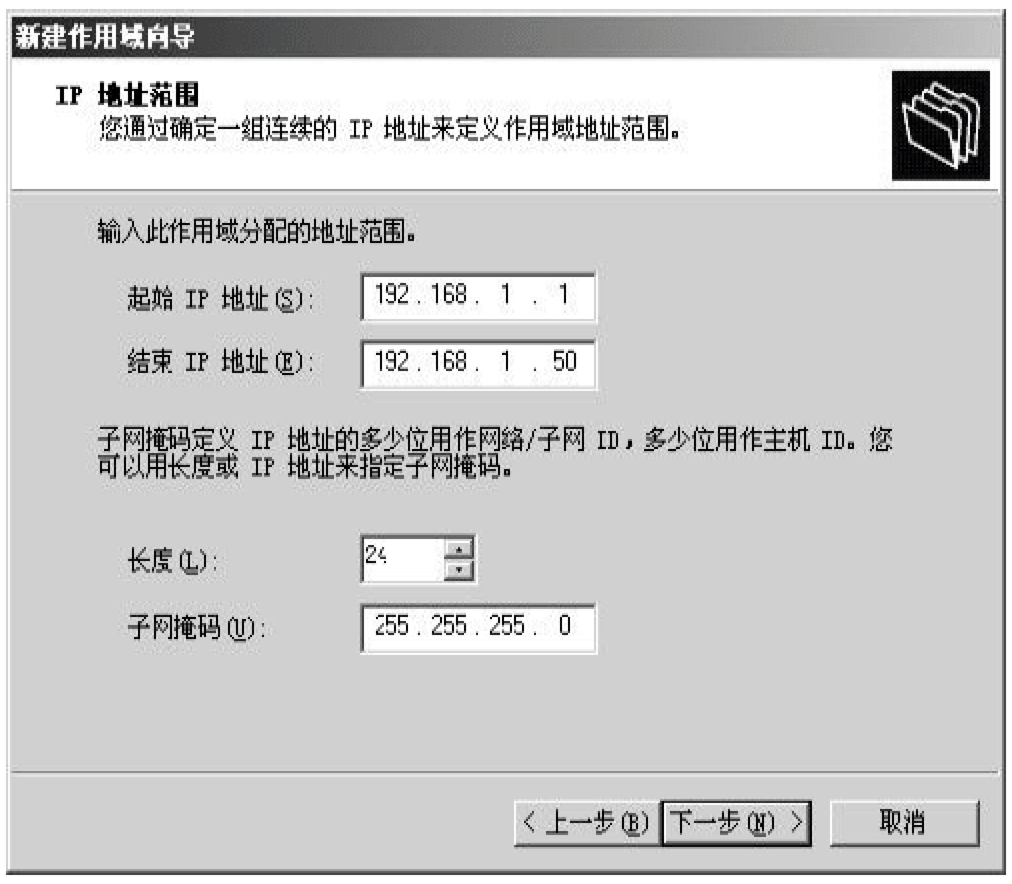


图 4-70　设置 IP 地址范围

(6) 设置好 IP 地址范围后，单击“下一步”按钮，打开“添加排除”向导页，如图 4-71 所示。这里用户可以指定前面设置的 IP 地址范围中有哪些地址不被服务器分配。如果想排除的 IP 地址是分散的，那么在“起始 IP 地址”中输入要排除的 IP 地址，然后单击“添

加”按钮，重复这一过程直至所有要排除的 IP 地址均被添加。如果想排除的是某一段连续的 IP 地址，则分别输入该范围的起始 IP 地址和结束 IP 地址，然后单击“添加”按钮。

(7) 单击“下一步”按钮，打开“租约期限”向导页，如图 4-72 所示。租约期限指的是一个客户端从此作用域使用 IP 地址的时间长短。通常局域网使用的都是专用保留 IP 地址，地址数量很充裕，所以可以将租约期限设置得较长。

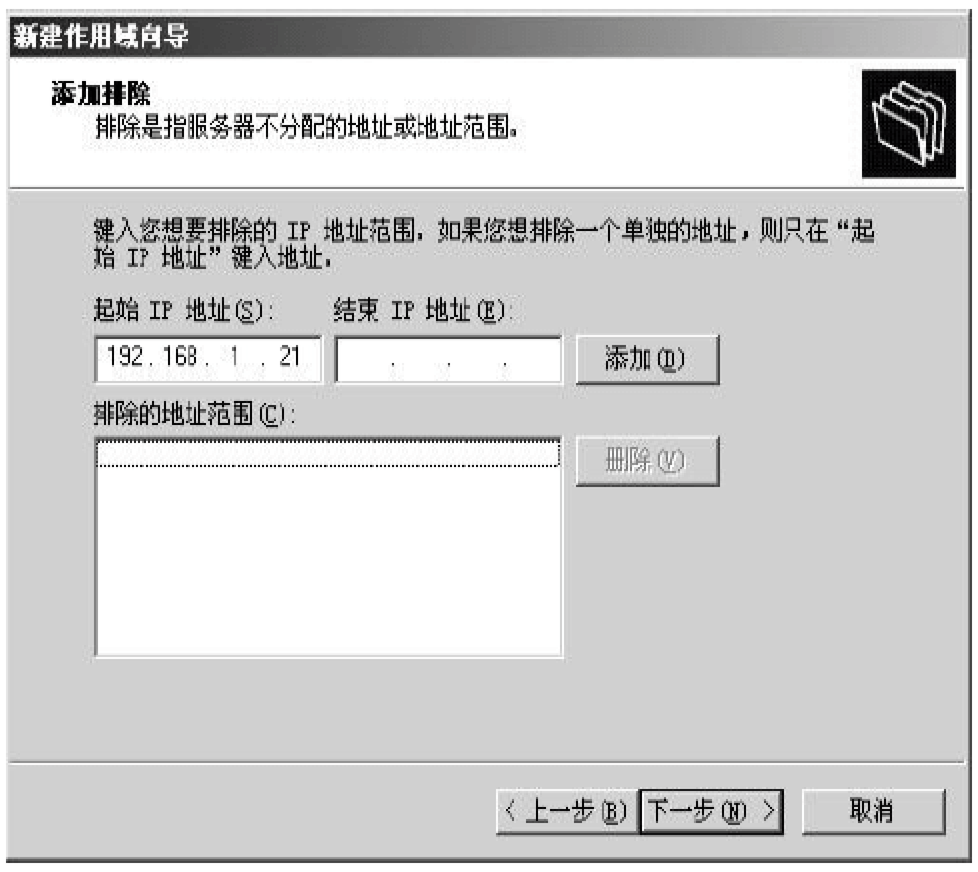


图 4-71 设置排除的 IP 地址

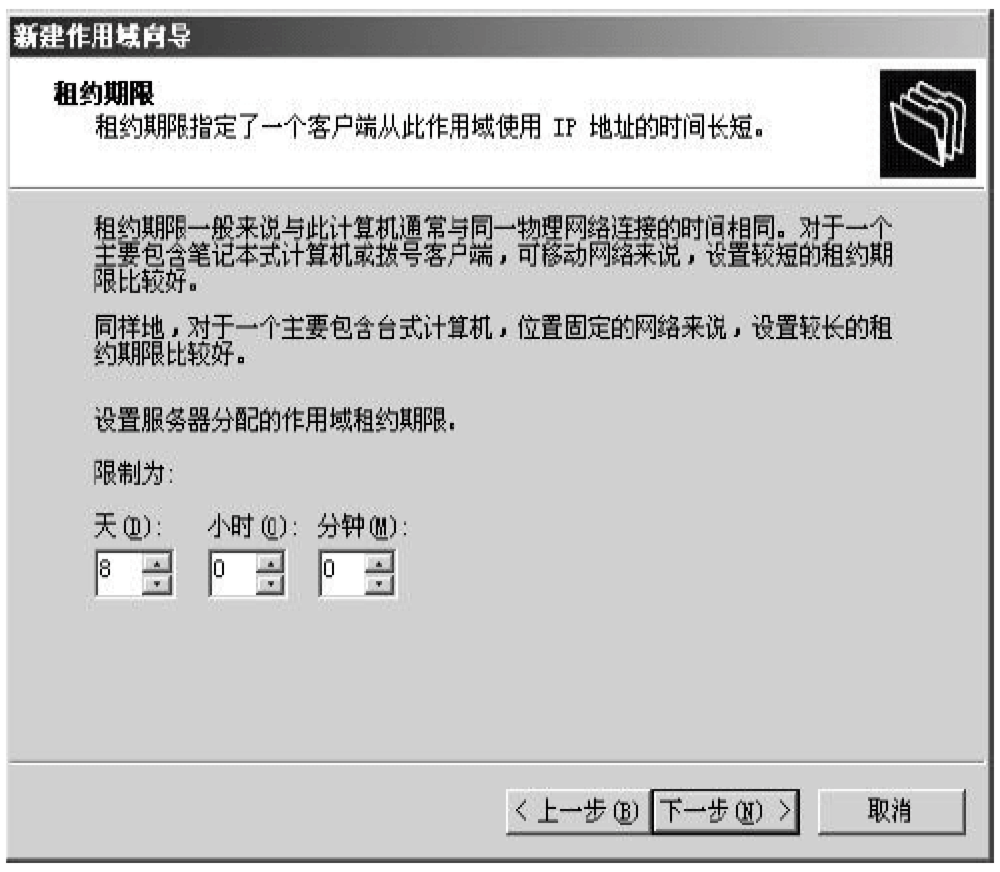


图 4-72 “租约期限”向导页

(8) 单击“下一步”按钮，向导提示用户为该作用域配置 DHCP 选项。通常只有正确配置了 DHCP 选项，DHCP 客户机才可以使用此作用域，所以选中“是，我想现在配置这些选项”单选按钮。

(9) 单击“下一步”按钮，首先要配置的是默认网关的 IP 地址。输入默认网关的 IP 地址，并单击“添加”按钮。

(10) 单击“下一步”按钮，接下来要配置的是域名称和 DNS 服务器。在“父域”文本框中输入域名，并在“IP 地址”文本框中输入 DNS 服务器的 IP 地址，然后单击“添加”按钮，如图 4-73 所示。若有多个 DNS 服务器，将其他的 DNS 服务器添加至此。通常设置两个 DNS 服务器即可，一个作为主 DNS 服务器，另一个作为辅 DNS 服务器。

(11) 单击“下一步”按钮，设置 WINS 服务器地址。如果网络中有 WINS 服务器，在“IP 地址”文本框中输入 WINS 服务器的地址，然后单击“添加”按钮，如图 4-74 所示。

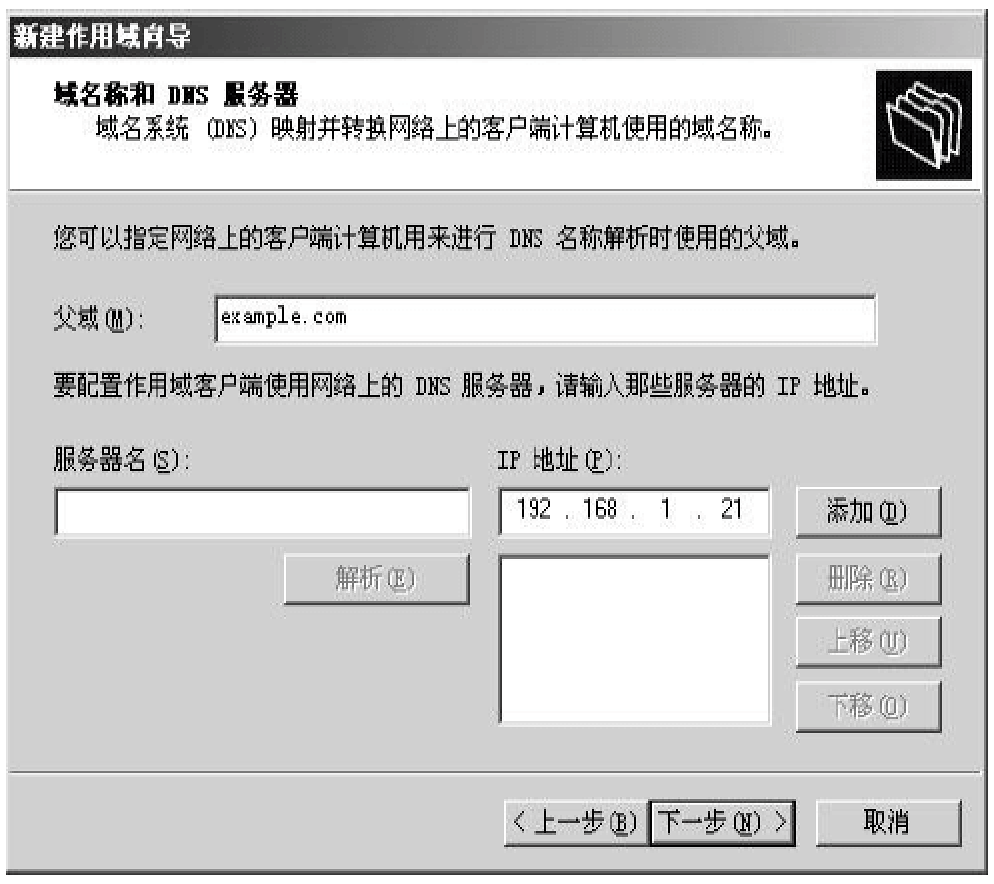


图 4-73 设置域名和 DNS 服务器

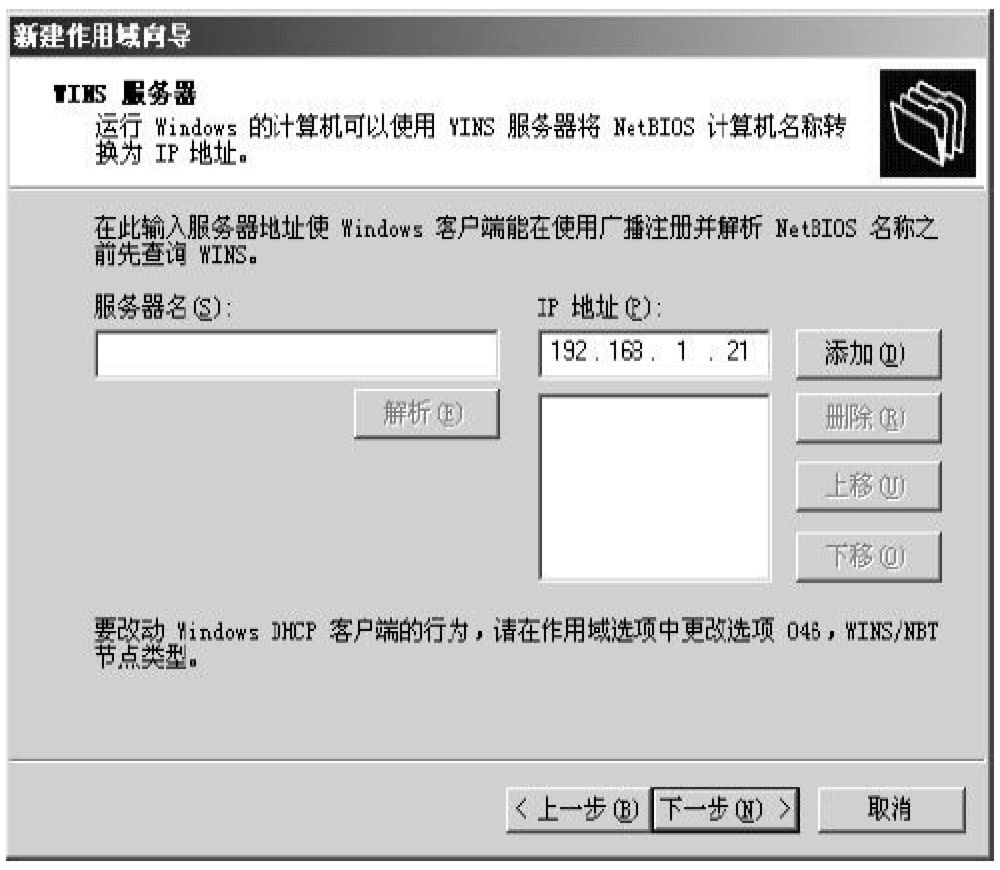


图 4-74 设置 WINS 服务器

(12) 单击“下一步”按钮，向导会提示是否激活此作用域，选择“是，我想现在激活此作用域”。

(13) 单击“下一步”按钮，向导提示已成功完成了新建作用域向导，单击“完成”按钮关闭向导。

接下来，系统会创建新的作用域。创建完成后的控制台如图 4-75 所示。展开新建的作用域，选择“地址池”选项，可以查看当前地址池中 IP 地址的范围及被排除的 IP 地址。选择“地址租约”选项，可以查看当前有哪些客户端租用了哪些 IP 地址。选择“保留”选项，可以查看并设置将地址池中的某些 IP 地址永久地分配给一些客户端。新建保留地址的方法是右键单击“保留”选项，在弹出的快捷菜单中选择“新建保留”命令，然后在弹出的对话框中输入相应的信息即可。需要注意的是，设置保留地址时，需要知道客户端网卡的 MAC 地址，即物理地址。网卡的物理地址可通过在“命令提示符”中运行 ipconfig /all 命令查看。

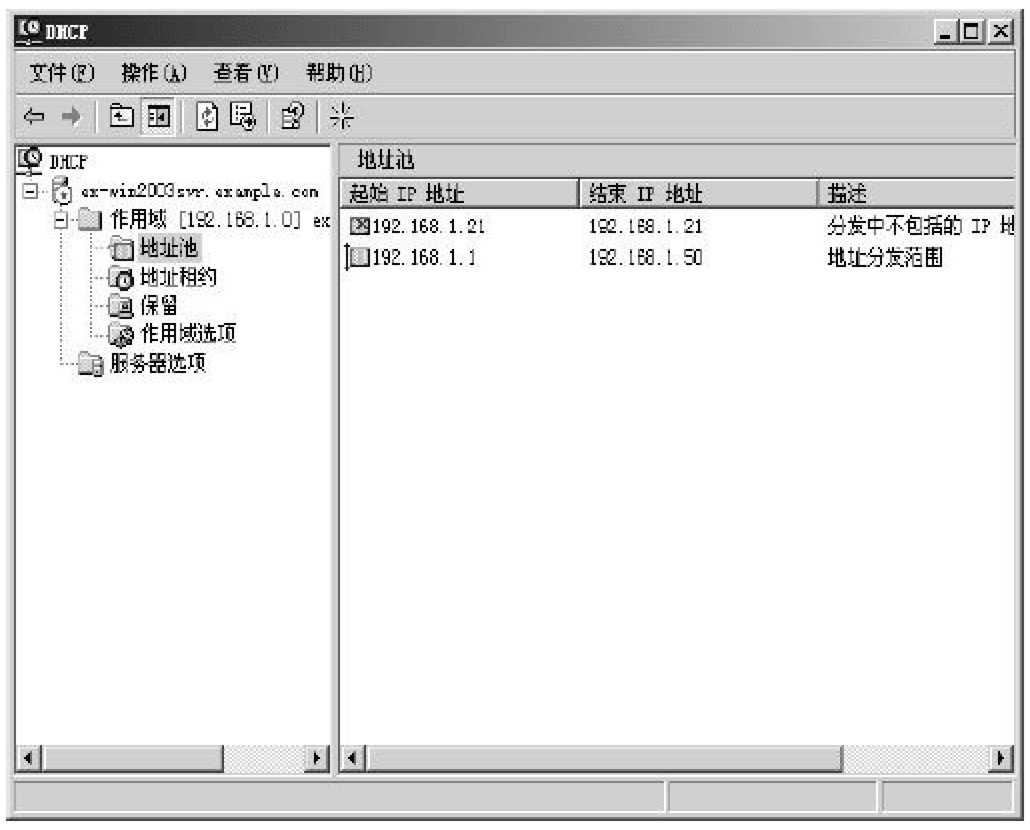


图 4-75　DHCP 服务器的地址池

选择“作用域选项”选项，可以查看当前为该作用域设置的选项，也就是前面新建作用域向导中所设置的路由器、域名、DNS 服务器和 WINS 服务器等信息。这些是保证客户端能正常访问网络所必需的信息。如果用户还需要为该作用域设置其他的附加选项，可右键单击“作用域选项”，在弹出的快捷菜单中选择“配置选项”命令，如图 4-76 所示。打开如图 4-77 所示的“作用域 选项”对话框，在“可用选项”中选中要设置的选项，并在下面设置相应的信息，然后单击“确定”按钮即可。

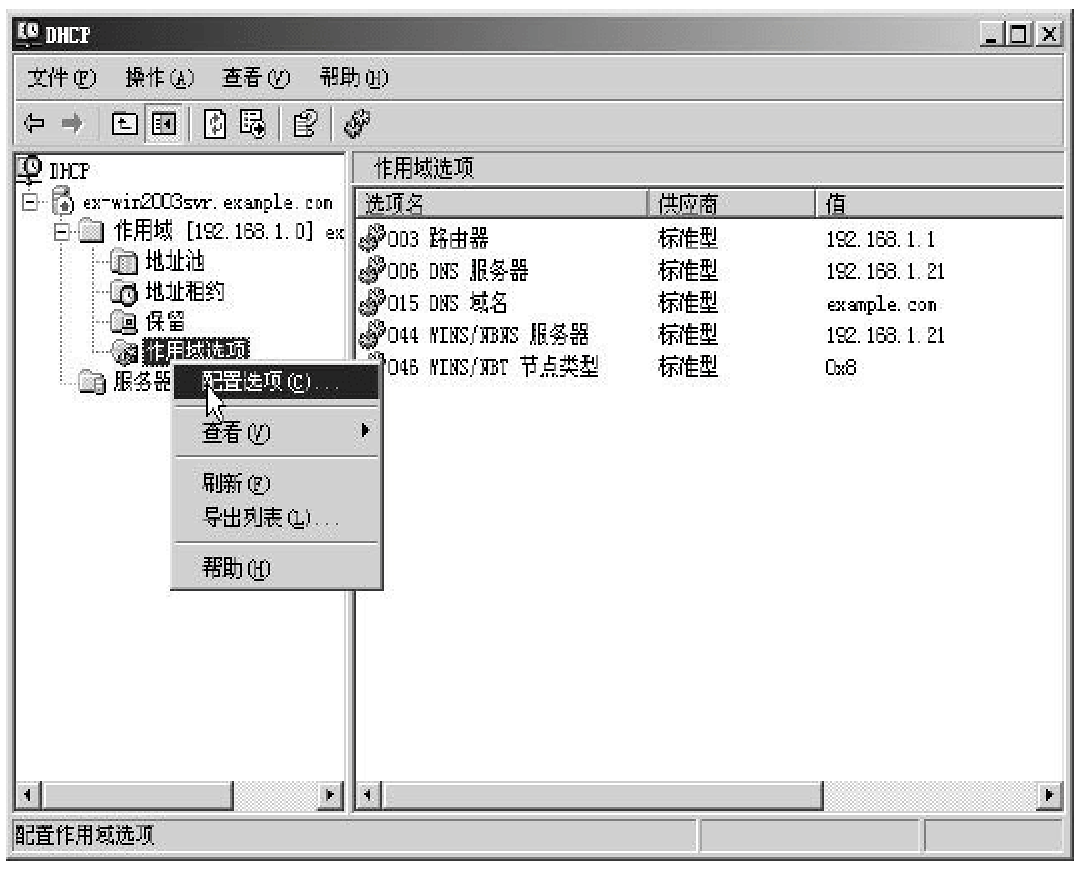


图 4-76　选择“作用域选项”→“配置选项”命令

图 4-77　“作用域 选项”对话框

右击新建的作用域，在弹出的快捷菜单中选择“属性”命令，可以对作用域的设置进行更改。作用域的属性对话框共有 3 个选项卡：“常规”、DNS 和“高级”选项卡。

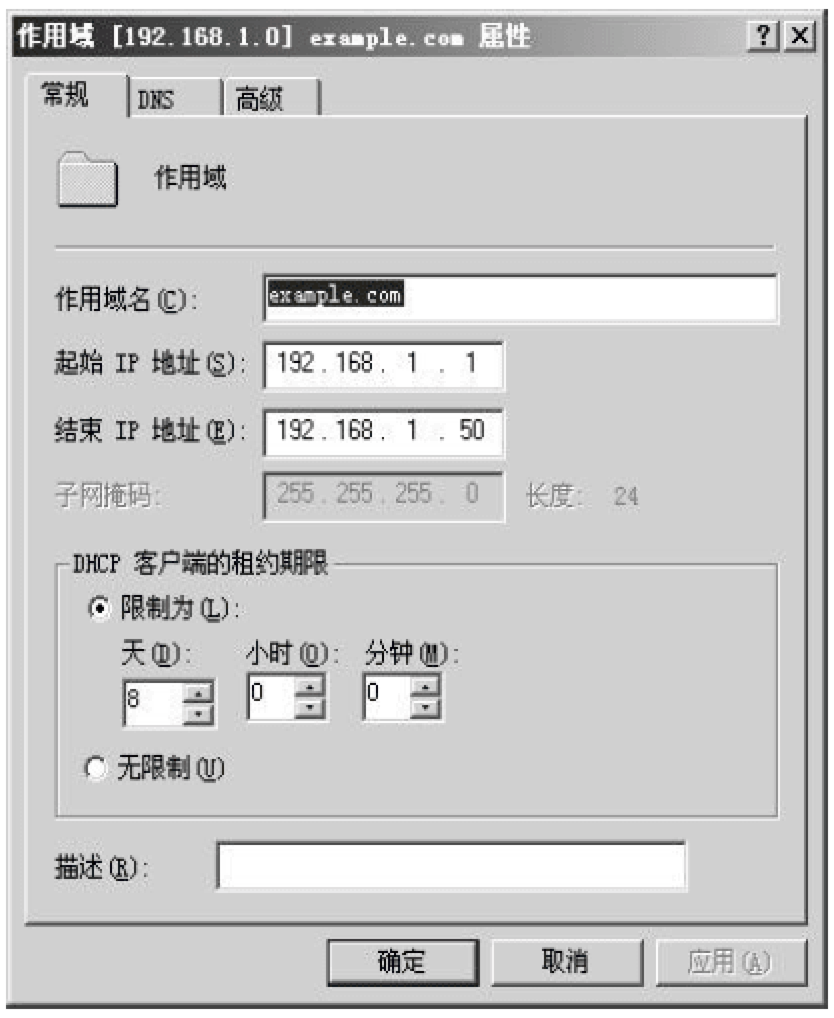


图 4-78 “常规”选项卡

“常规”选项卡如图 4-78 所示，在此可以更改作用域名、IP 地址范围和租约期限。

DNS 选项卡可以设置 DHCP 服务器是否启用 DNS 动态更新。启用 DNS 动态更新的好处是当客户端的 IP 地址发生变化后，DHCP 服务器将会发送信息更新 DNS 服务器中的主机和指针记录，以确保信息的一致性。

“高级”选项卡可以指定 DHCP 服务器为哪种类型的客户端动态分配 IP 地址，其中 BOOTP 一般为无盘工作站客户端，若网内没有无盘工作站，选择“仅 DHCP”选项即可。

当安装 DHCP 服务器的计算机同时也是域控制器时，在使用 DHCP 服务器前需对其进行授权，这是因为当错误配置或未授权的 DHCP 服务器被引入网络时，可能会引发问题。例如，如果启动了未授权的 DHCP 服务器，它可能会为客户端租用不正确的 IP 地址或者否认尝试续订当前地址租约的 DHCP 客户端。这两种配置中的任何一个都可能导致启用 DHCP 的客户端产生更多的问题。例如，从未授权的服务器获取配置租约的客户端将找不到有效的域控制器，从而导致客户端无法成功登录到网络。为了避免这些问题，在客户端之前运行 Windows Server 2008 R2 上的 DHCP 服务器服务时，需要验证是否已在 Active Directory 中对它们进行了授权。这样就避免了由于运行带有不正确配置的 DHCP 服务器或者在错误的网络上运行配置正确的服务器而导致的大多数意外破坏。DHCP 服务器一旦在授权列表中发现其 IP 地址，便进行初始化并开始为客户端提供 DHCP 服务。如果在授权列表中未发现自己的地址，则不进行初始化并停止提供 DHCP 服务。

授权的某台 DHCP 服务器的操作方法如下：依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。右键单击要授权的服务器名，在弹出的快捷菜单中选择“授权”命令。授权过程需要一段时间，期间用户可以按 F5 键查看状态，检查是否完成授权。

要解除某台已授权服务器的授权，方法与授权过程相同，只是在弹出的快捷菜单中选择“撤销授权”命令。

4.3.2 典型例题分析

例 1 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】某学校的图书馆电子阅览室已经连接成为局域网(局域网段为 192.168.1.0/24/)，在原有接入校园网的基础上又租用了电信的 ADSL 宽带接入来满足用户的上网需求。其中，校园网网段为 210.27.176.0～210.27.191.255，DNS 为 210.27.176.3，子网按照 C 类网络划分，每个子网的网关都为 210.27.XXX.1。ADSL 宽带的网络地址由电信自动分配，具体网络结构如图 4-79 所示。

【问题 1】(6 分)

如图 4-79 所示，在该电子阅览室网络的出口利用了一台安装 Windows Server 2003 的服务器实现客户机既能访问本校和本馆内的电子资源，又能够通过 ADSL 访问外部资源。现计划在 Sever1 上安装 3 块网卡来实现这个功能，三块网卡首先需要在如图 4-80 所示的对话框中配置 IP 地址等信息。按照题目要求选择(1)～(6)中的正确选项。

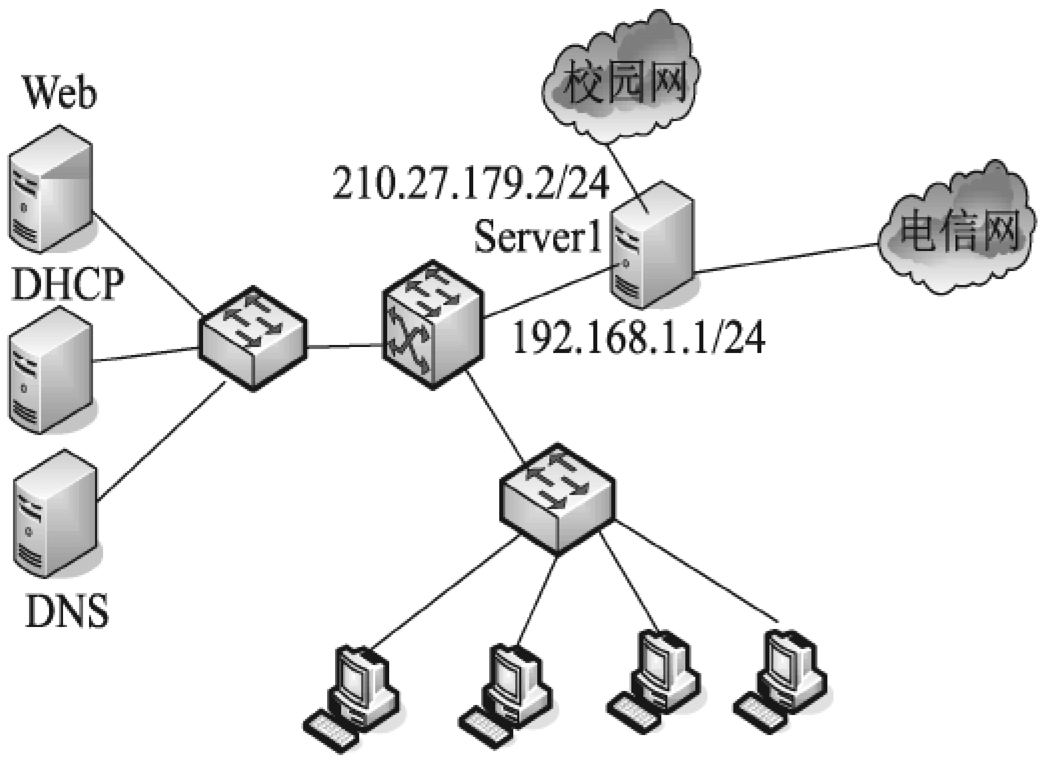


图 4-79　网络拓扑结构图

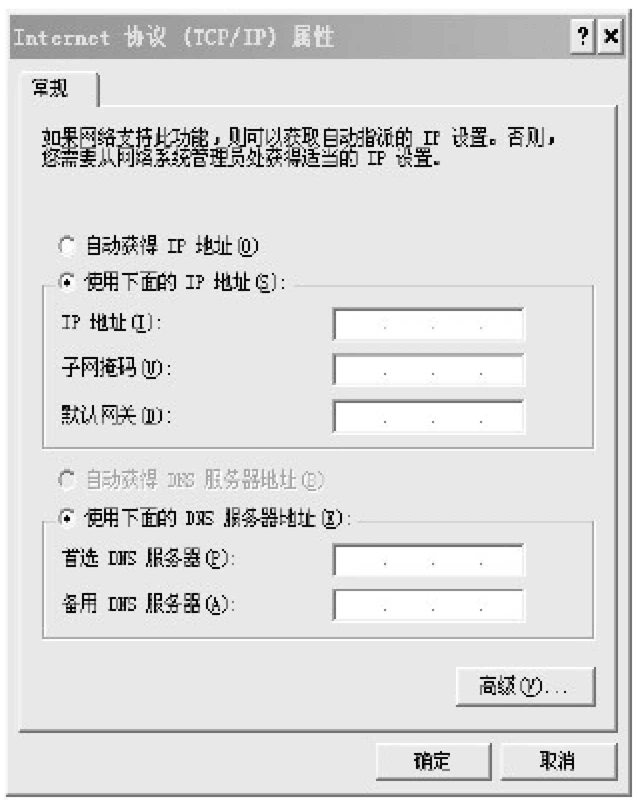


图 4-80　“Internet 协议(TCP/IP)属性”对话框

网卡 1：连接电子预览室内网，IP 地址：192.168.1.1，子网掩码为 255.255.255.0，网关 (1) ，DNS (2) 。

网卡 2：连接 ADSL 电信网，IP 地址： (3) ，DNS (4) 。

网卡 3：连接校园网，IP 地址： (5) ，子网掩码为 255.255.255.0，网关为 (6) ，DNS 为 210.27.176.3。

空(1)～(6)备选答案：

A. 192.168.1.1　　B.自动获取　　C. 192.168.1.2　　D. 不指定，保持为空

E. 210.27.179.2　　F. 210.27.179.1　　G. 255.255.255.0

【问题 2】(8 分)

在 Sever1 上开启路由和远程访问服务，出现如图 4-81 所示的窗口，在继续配置“网络接口”时，出现如图 4-82 所示的对话框，应该选择“ (7) ”，然后选择 ADSL 账号和密码完成连接建立过程。

图 4-81　“路由和远程访问”窗口

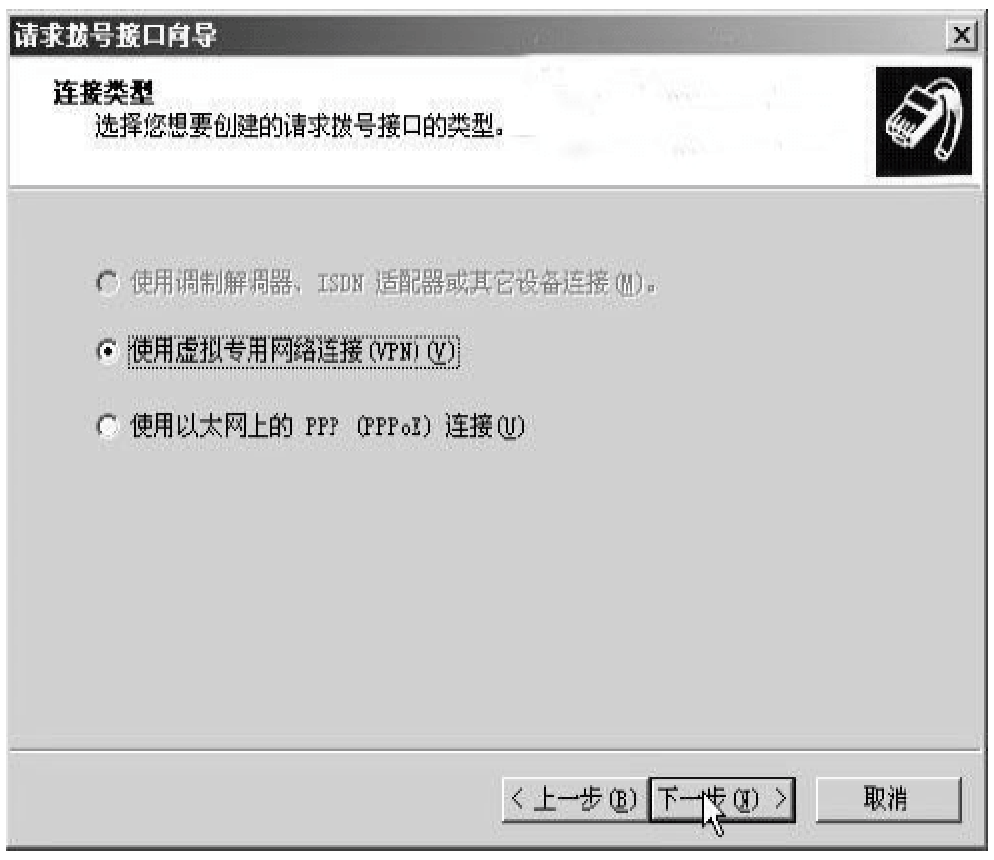


图 4-82　“请求拨号接口向导”对话框

为了使客户机自动区分电子预览室内网、校园网和 ADSL 电信网，还需新建一个批处理文件 route.bat，并把路由功能加入到服务器中，route.bat 文件内容如下所示，完成相关配置。

```
cd\
route delete _(8)_    //删除默认路由
route add _(9)_ mask 255.255.255.0 192.168.1.1  //定义内网路由
route add _(10)_ mask  255.255.255.0 210.27.176.1
 //定义校园网一个网段路由
…//依次定义校园网其他各网段路由
```

【问题 3】(2 分)

因为电子阅览室的 DHCP 服务器老化需要更换，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这是采用导入导出的方式进行配置的迁移，采用的步骤如下。

1. 在原有的DHCP服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt”命令，将该文件复制到新服务器的相同位置。

2. 在新的服务器上安装好 DHCP 服务器后，在命令行模式下输入“_(11)_”命令，即可完成 DHCP 服务器的迁移。

3. 在迁移操作时，一定要使用系统_(12)_组的有效账户。

【问题 4】(4 分)

1. 若电子阅览室的客户机访问 Web 服务器时出现“HTTP 错误：401.1-未经授权：访问由于凭据无效被拒绝。”现象，则需要在“控制面板”→“管理工具”→“计算机管理”→“本地用户和组”，将_(13)_账号启用来解决此问题。

2. 若出现“HTTP 错误：401.2-未经授权：访问由于服务器配置被拒绝。”现象，造成该错误的原因是身份验证设置的问题，一般应将其设置为_(14)_身份认证。

空(13)、(14)备选答案：

A. IUSR_机器名　　B. Administrator　　C. Guest　　D. 匿名

答案：

【问题 1】

(1) D　(2) D　(3) B　(4) B　(5) E　(6) F

【问题 2】

(7)使用以太网上的 PPP(PPPoE)连接　(8) 0.0.0.0　(9)192.168.1.0　(10) 210.27.176.0

【问题 3】

(11) netsh dhcp server import　c:\dhcpbackup.txt　(12) 管理员

【问题 4】

(13) A　(14) D

解析：

【问题 1】 由题知，网卡 1 连接电子预览室内网，IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，故网关和 DNS 均为不指定，保持为空。

网卡 2 连接 ADSL 电信网，因为 ADSL 宽带的网络地址由电信自动分配，故 IP 地址和

DNS 自动分配。

网卡 3 连接校园网，IP 地址为 210.27.179.2，网关为 210.27.179.1。其中，校园网网段为 210.27.176.0～210.27.191.255，DNS 为 210.27.176.3。由网络结构图知，IP 地址为 210.27.179.2。

【问题 2】 在 Severl 上开启路由和远程访问服务，出现如图 4-81 所示的窗口，在继续配置“网络接口”时，出现如图 4-82 所示的对话框，应该选择“使用以太网上的 PPP(PPPoE)连接”，然后选择 ADSL 账号和密码完成连接建立过程。

route delete 0.0.0.0 为了删除默认路由。route add 192.168.1.0 mask 255.255.255.0 192.168.1.1 为了添加下面的内网路由。由题知，校园网网段为 210.27.176.0～210.27.191.255，DNS 为 210.27.176.3，接着定义校园网一个网段路由 210.27.176.0，route add 210.27.176.0 mask 255.255.255.0 210.27.176.1。

【问题 3】 在 Windows Server 2003 Netsh.exe 中包含两个命令可为动态主机配置协议(DHCP)：导出和导入。这些命令可用于有选择地导出和导入 DHCP 作用域。

1. 在原有的 DHCP 服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt”命令，将该文件复制到新服务器的相同位置。

2. 在新的服务器上安装好 DHCP 服务器后，在命令行模式下输入“netsh dhcp server import c:\dhcpbackup.txt”命令，即可完成 DHCP 服务器的迁移。

3. 在迁移操作时，一定要使用系统管理员组的有效账户。

【问题 4】

1. 若电子阅览室的客户机访问 Web 服务器时出现“HTTP 错误：401.1-未经授权：访问由于凭据无效被拒绝。”现象，则需要在“控制面板”→“管理工具”→“计算机管理”→“本地用户和组”，将 IUSR_机器名账号启用来解决此问题。

错误号：401.1

症状：HTTP 错误 401.1 - 未经授权：访问由于凭据无效被拒绝。

分析：由于用户匿名访问使用的账号(默认是 IUSR_机器名)被禁用，或者没有权限访问计算机，将造成用户无法访问。

解决方案：请尝试用以下办法启用：“控制面板”→“管理工具”→“计算机管理”→“本地用户和组”，将 IUSR_机器名账号启用。

2. 若出现“HTTP 错误：401.2-未经授权：访问由于服务器配置被拒绝。”现象，造成该错误的原因是身份验证设置的问题，一般应将其设置为匿名身份认证。

错误号：401.2

症状：HTTP 错误 401.2-未经授权：访问由于服务器配置被拒绝。

原因：关闭了匿名身份验证解决方案：运行 inetmgr，打开站点属性→目录安全性→身份验证和访问控制，选中“启用匿名访问”，输入用户名，或者单击“浏览”按钮选择合法的用户，并两次输入密码后确定。

例 2　某单位网络拓扑结构如图 4-83 所示，该单位 Router 以太网接口 E0 接内部交换机 S1，S0 接口连接到电信 ISP 的路由器；交换机 S1 连接内部的 Web 服务器、DHCP 服务器、DNS 服务器和部分客户机，服务器均安装 Windows Server 2003，办公室的代理服务器(Windows XP 系统)安装了两块网卡，分别连接交换机 S1、S2，交换机 S1、S2 的端口均在

VLAN1 中。

【问题 1】(4 分)

根据图 4-83，该单位 Router S0 接口的 IP 地址应设置为_(1)_；在 S0 接口与电信 ISP 路由器接口构成的子网中，广播地址为_(2)_。

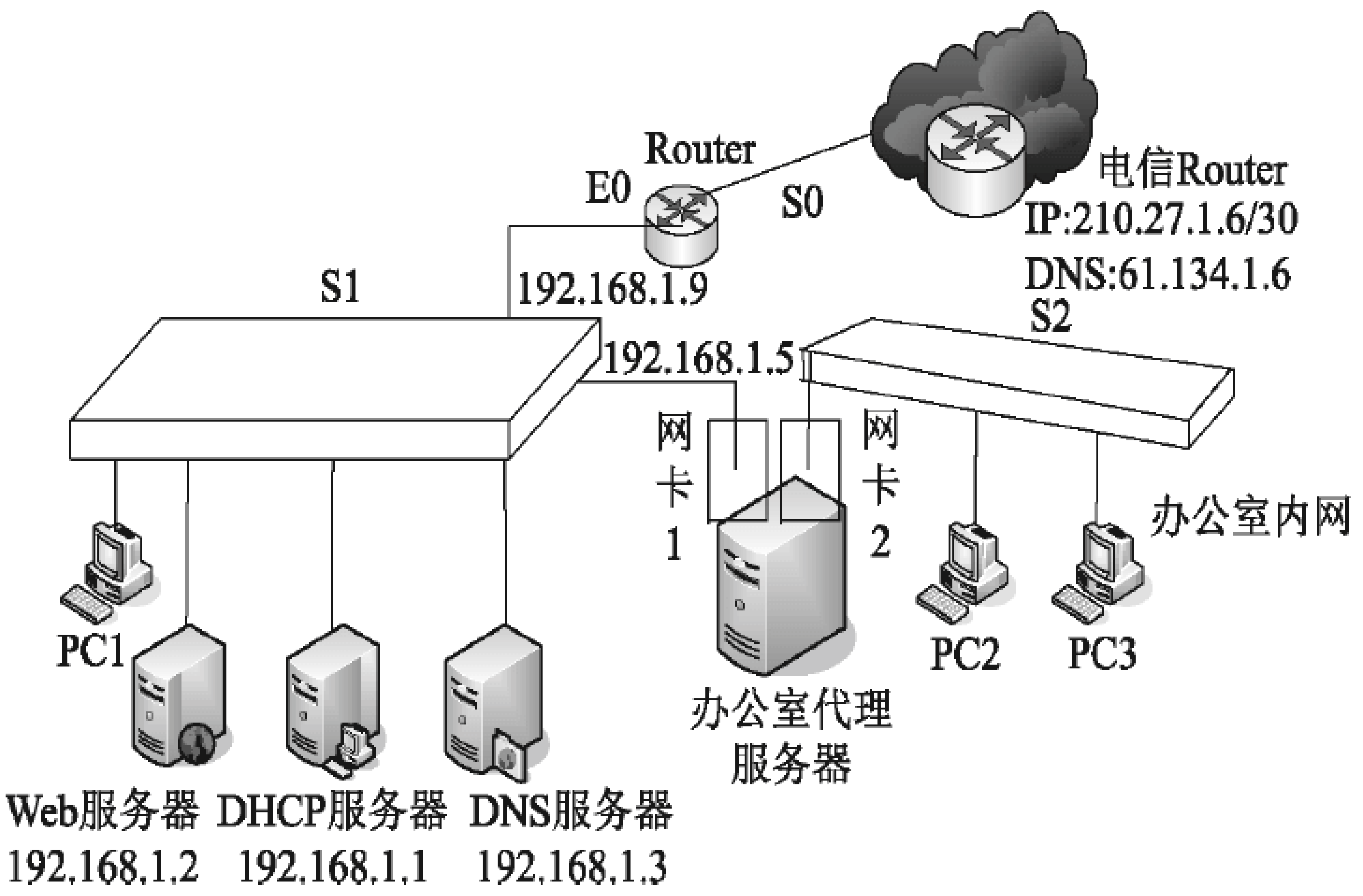


图 4-83　网络拓扑结构图

【问题 2】(2 分)

办公室代理服务器的网卡 1 为静态地址，在网卡 1 上启用 Windows XP 内置的“Internet 连接共享”功能，实现办公室内网的共享代理服务；那么通过该共享功能自动分配给网卡 2 的 IP 地址是_(3)_。

【问题 3】(2 分)

在 DHCP 服务器的安装过程中，租约期限一般默认为_(4)_天。

【问题 4】(2 分)

该单位路由器 Router 的 E0 口设置为 192.168.1.9/24，若在 DHCP 服务器上配置、启动、激活 DHCP 服务后，查看 DHCP 地址池的结果如图 4-84 所示。

图 4-84　DHCP 地址池

为了满足图 4-83 的功能，在 DHCP 服务器地址池配置操作中还应该增加什么操作?

【问题 5】(3 分，每空 1 分)

假如在图 4-84 中移除 DHCP 服务器，改由单位 Router 来提供 DHCP 服务，在 Router 上配置 DHCP 服务时用到了如下命令，请在下画线处将命令行补充完整。

```
Router(config)#ip__(5)__hkhk//配置 DHCP 地址池名为 hkhk
Router(dhcp-config)#__(6)__192.168.1.0   255.255.255.0
Router(dhcp-config)#__(7)__192.168.1.9
```

【问题 6】(4 分，每空 2 分)

如图 4-85 所示，在 QQQ 网站的属性对话框中，若“网站”选项卡的“IP 地址”设置为“全部未分配”，则说明__(8)__。

(8)备选答案：

A. 网站的 IP 地址为 192.168.1.1，可以正常访问

B. 网站的 IP 地址为 192.168.1.2，可以正常访问

C. 网站的 IP 地址未分配，无法正常访问

在图 4-86 的 Web 服务“主目录”选项卡上，至少要设置对主目录的__(9)__权限，才能访问该 Web 服务器。

(9)备选答案：

A. 读取　　B. 写入　　C. 目录浏览　　D. 记录访问

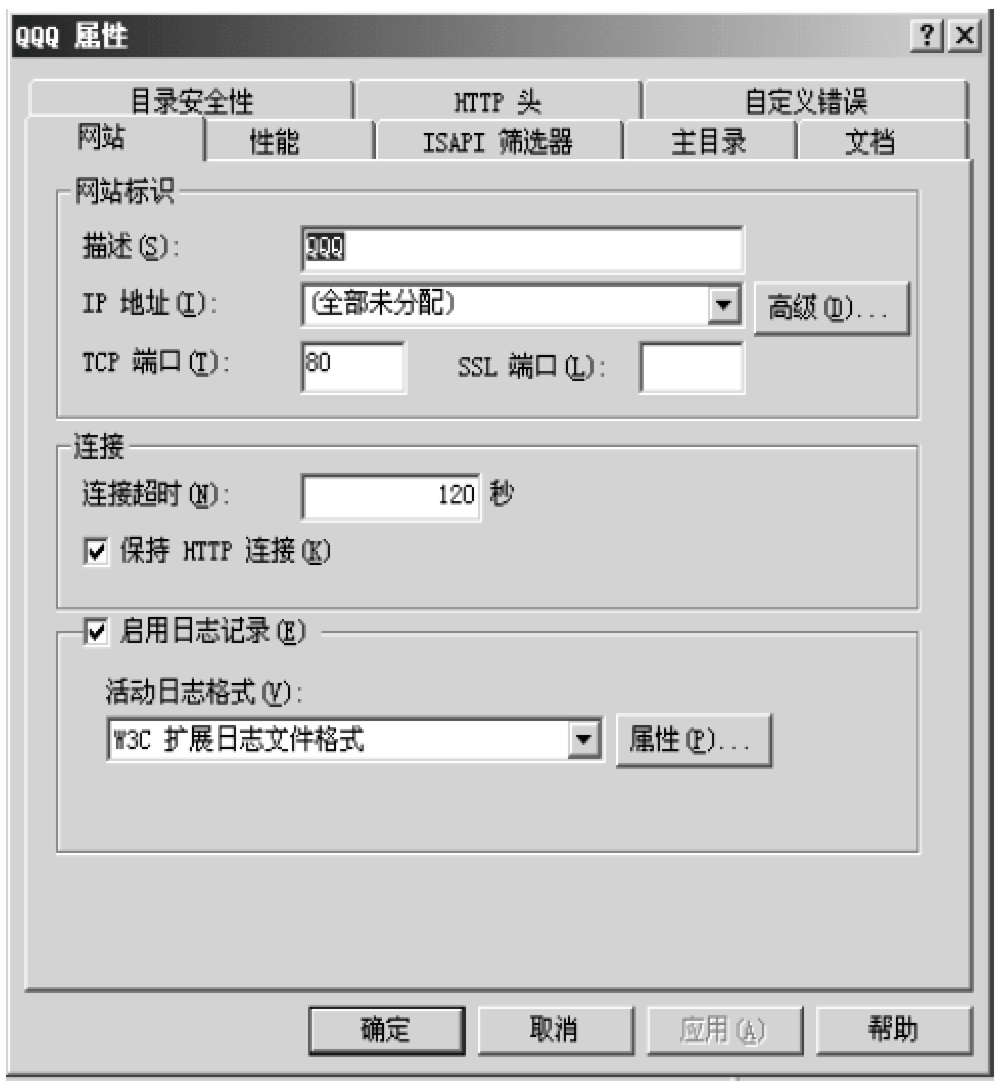


图 4-85　“网站”选项卡

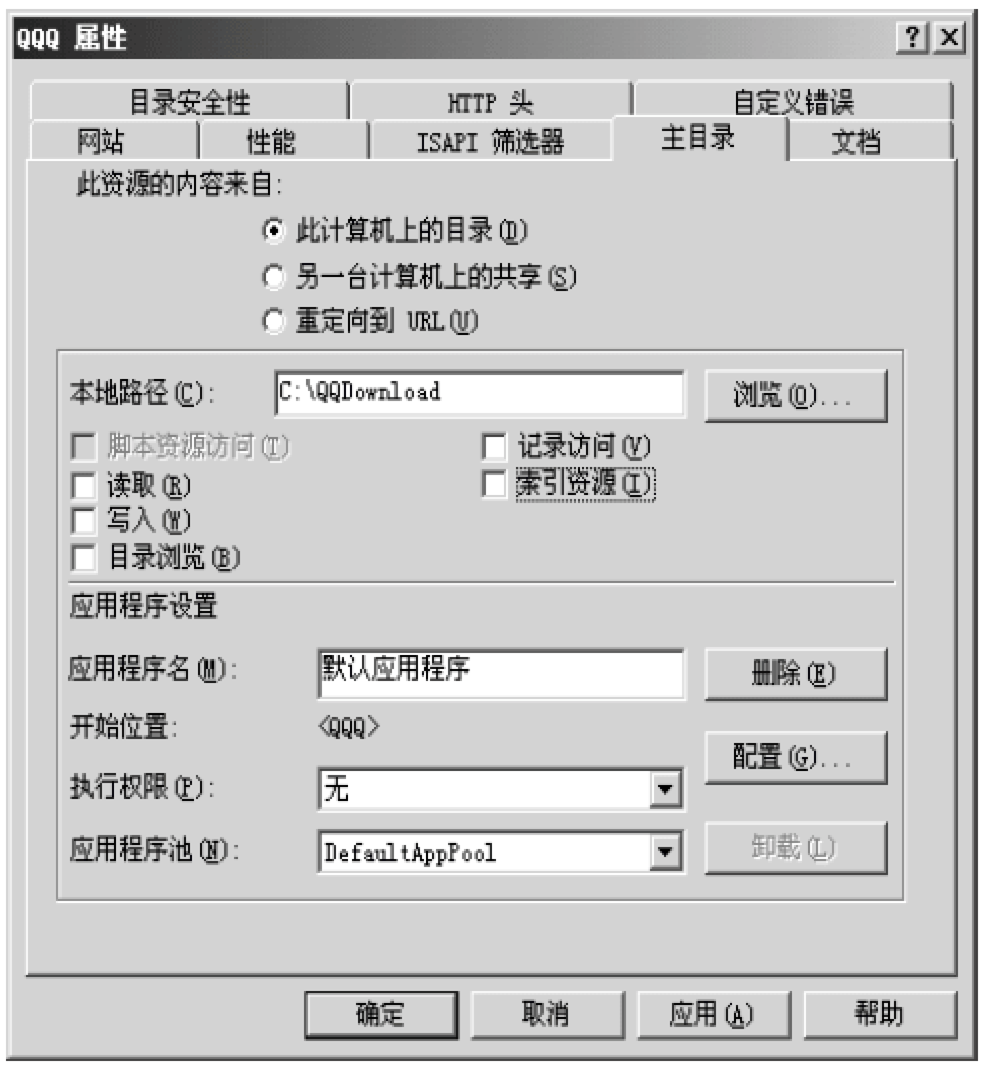


图 4-86　“主目录”选项卡

【问题 7】(3 分)

按系统默认的方式配置了 KZ 和 QQQ 两个网站(如图 4-87 所示)，此时两个网站均处于停止状态，若要使这两个网站能同时工作，请给出三种可行的解决办法。

方法一：__(10)__。

方法二：__(11)__。

方法三：__(12)__。

图 4-87　KZ 和 QQQ 网站配置

答案：

【问题 1】

(1) 210.27.1.5　(2) 210.27.1.7

【问题 2】

(3) 192.168.0.1

【问题 3】

(4) 8

【问题 4】

进行“添加排除”IP 地址的操作

【问题 5】

(5) dhcp pool　(6) network　(7) default-router

【问题 6】

(8) B　(9) A

【问题 7】

(10) 给 KK 和 QQQ 指定不同的 IP 地址

(11) 给 KK 和 QQQ 指定不同的主机头值

(12) 给 KK 和 QQQ 指定不同的端口号

解析：

【问题 1】 由电信 Router 的 IP 地址 210.27.1.6/30 可知，主机号为 2 位，写成二进制为 201.27.1.0000 0110，主机号全为 1 时为广播地址，即 210.27.1.0000 0111，故广播地址为 210.27.1.7；将最后 2 位改成 01，即可得到 Router S0 接口的 IP 地址为 210.27.1.5。

【问题 2】 网卡 1 通过共享，自动分配给网卡 2 的 IP 地址即 192.168.0.1

【问题 3】 DHCP 服务器租约(默认情况是 8 天)。

【问题 4】 缺少“添加排除”页面，这里用户可以指定前面设置的 IP 地址范围中有哪些地址不被服务器分配。

【问题 5】 空(5)处是配置 DHCP 地址池名，故填 dhcp pool；空(6)处填 network；空(7)处配置默认路由。

【问题 6】IP 地址设为全部未分配，由图 4-83 可知 Web 服务器的 IP 地址为 192.168.1.2，

可以正常访问。要访问 Web 服务器，必须设置对主目录的读取权限。

【问题 7】 要使两个网站能同时工作可以采用以下方法：给 KK 和 QQQ 指定不同的 IP 地址；给 KK 和 QQQ 指定不同的主机头值；给 KK 和 QQQ 指定不同的端口号。

例 3　阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】某网络拓扑结构如图 4-88 所示，网络 1 和网络 2 的主机均由 DHCP_Server 分配 IP 地址。FTP_Server 的操作系统为 Windows Server 2003，Web_Server 的域名为 www.softexamtest.com。

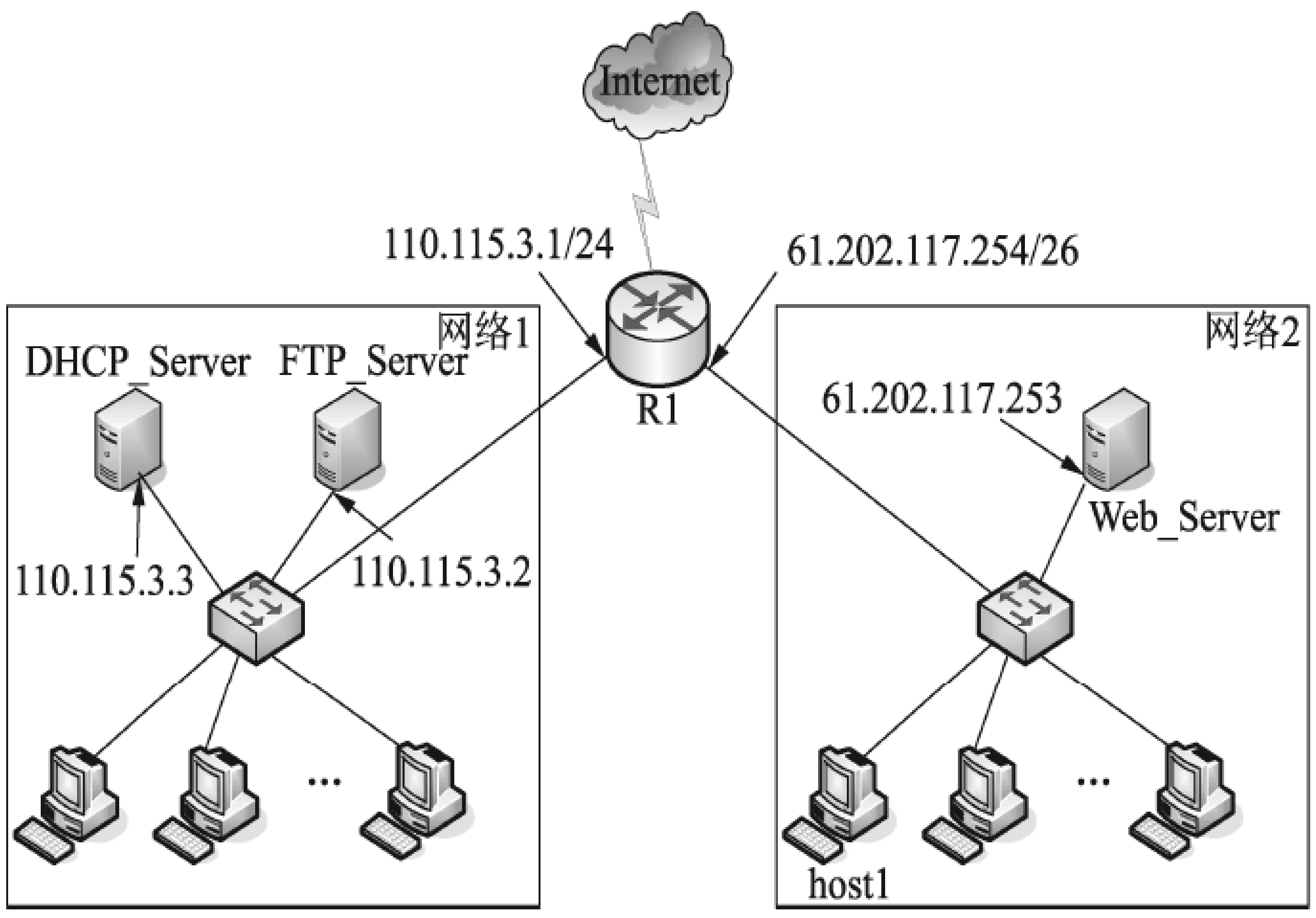


图 4-88　网络拓扑结构图

【问题 1】(4 分)

DHCP_Server 服务器可以动态分配的 IP 地址范围为__(1)__和__(2)__。

【问题 2】(2 分)

若在 host1 上运行 ipconfig 命令，可获得如图 4-89 所示结果，host1 能正常访问 Internet 吗？说明原因。

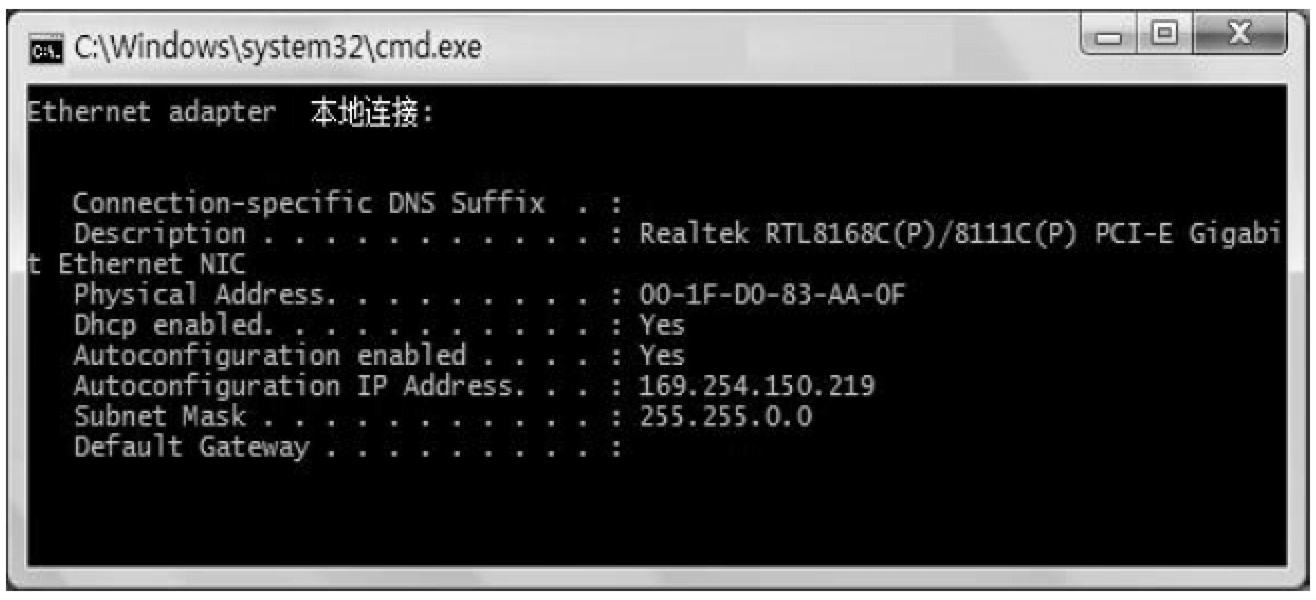


图 4-89　ipconfig 命令的执行结果

【问题 3】(3 分)

若 host1 成功获取 IP 地址后，在访问 http://www.abc.com 网站时，总是访问到 www.softexamtest.com，而同一网段内的其他客户端访问该网站正常。在 host1 的 C:\Windows\system32\drivers\etc 目录下打开__(3)__文件，发现其中有以下两条记录：

```
127.0.0.1   localhost
  (4)     www.abc.com
```

在清除第 2 条记录后关闭文件，重启系统或 host1 访问 http://www.abc.com 网站正常。请填充(4)处空缺的内容。

【问题 4】(2 分)

在配置 FTP_Server 时，图 4-90 的“IP 地址”文本框中应填入__(5)__。

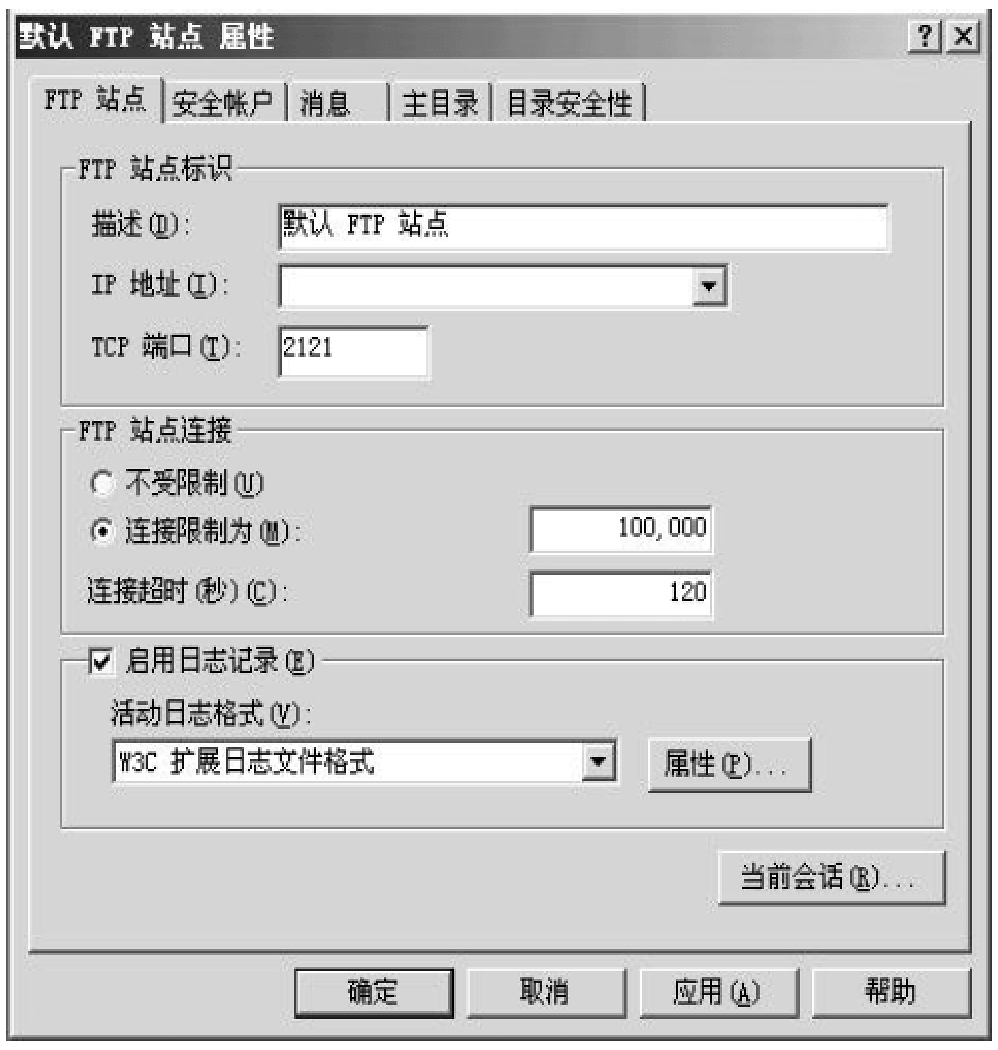


图 4-90　FTP_Server 的配置

【问题 5】(4 分)

若 FTP 配置的虚拟目录为 pcn，虚拟目录配置如图 4-91 和图 4-92 所示。

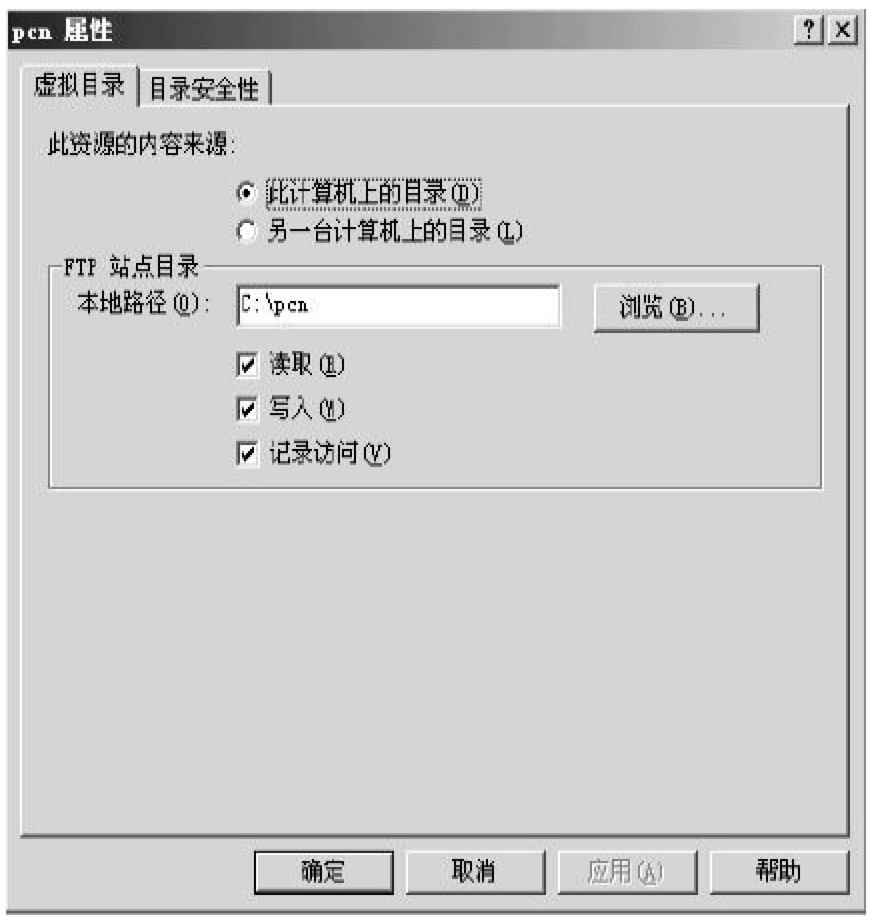


图 4-91　“虚拟目录”选项卡

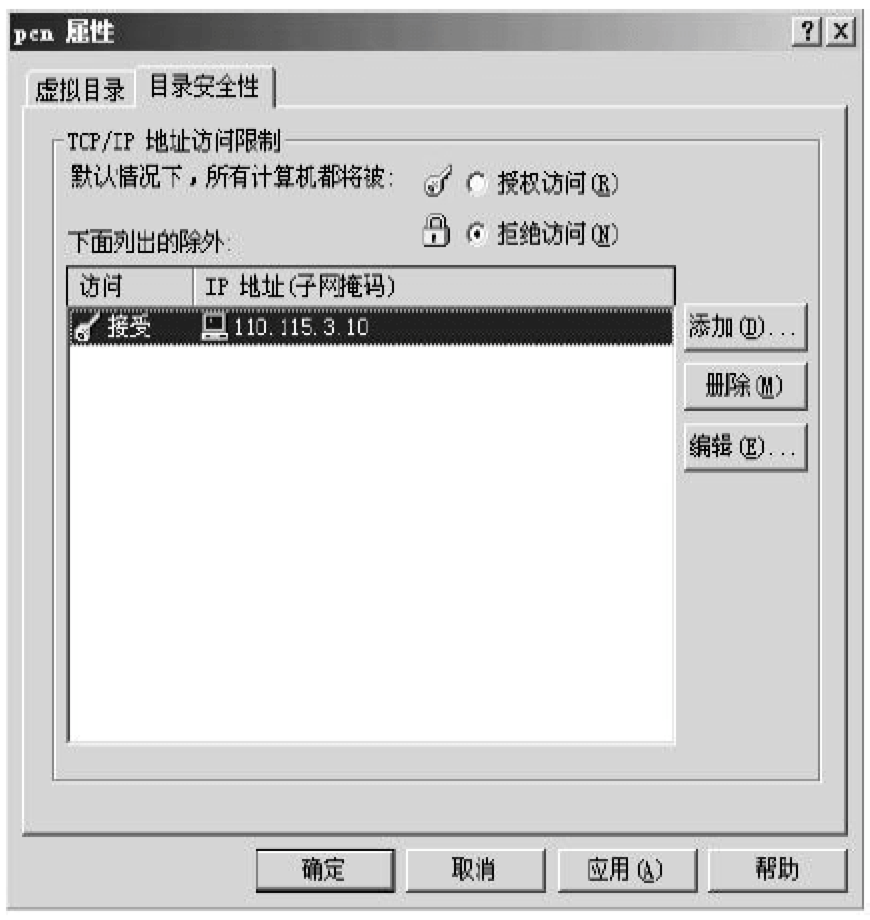


图 4-92　“目录安全性”选项卡

根据以上配置，哪些主机可以访问该虚拟目录？访问该虚拟目录的命令是__(6)__。

答案：

【问题 1】

(1) 110.115.3.4～110.115.3.254　(2) 61.202.117.193～61.202.117.252

注意：(1)和(2)的内容可以调换。

【问题 2】

host1 不能正常访问 Internet。因为它的 IP 地址属于 169.254.0.0/16 这个 B 类网段，表明它没有从 DHCP 服务器成功获取到一个有效的 IP 地址。

【问题 3】

(3) hosts　(4) 61.202.117.253

【问题 4】

(5) 110.115.3.2

【问题 5】

(6) ftp://110.115.3.2:2121/ 或 ftp://110.115.3.2:2121/pcn

解析：

【问题 1】 本题考查 DHCP 服务器的配置。从图 4-88 中可以看出 110.115.3.1、110.115.3.2、110.115.3.3 分别已经固定给了路由器和两台服务器，所以地址范围为 110.115.3.4～110.115.3.254。

【问题 2】当客户端未能从 DHCP 服务器获得 IP 地址时，客户端会检查自己是否配置了备用 IP 地址。如果配置了备用 IP 地址，那么客户端会首先启用备用 IP 地址；如果没有配置备用 IP 地址，客户机将从 169.254.0.0/16 这个 B 类网段中选择一个作为 IP 地址，并且每隔 5 分钟就再次进行 DHCP 地址申请。

【问题 3】 本题考查 DHCP 服务器的配置，打开 hosts 文件可查看记录。Hosts 是静态的 IP 和域名映射的关系。

【问题 4】 本题考查 FTP 服务器的配置，填写需要配置的 IP 地址。看图即可，此处还可以填写“所有未分配 IP”。

【问题 5】只有 110.115.3.10 这台主机可以访问该虚拟目录。所以命令为 ftp://110.115.3.2:2121/ 或 ftp://110.115.3.2:2121/pcn。

4.3.3　同步练习

阅读以下关于动态主机配置协议(DHCP)的说明，回答问题 1 至问题 4。

【说明】在小型网络中，IP 地址的分配一般都采用静态方式，需要在每台计算机上手工配置网络参数，诸如 IP 地址、子网掩码、默认网关和 DNS 等。在大型网络中，采用 DHCP 完成基本网络配置会更有效率。

【问题 1】(每空 1 分，共 4 分)

请在(1)～(4)空白处填写恰当的内容。

DHCP 的工作过程是：

1. IP 租用请求。DHCP 客户机启动后，发出一个 DHCPDISCOVER 消息，其封包的源地址为 (1) ，目标地址为 (2) 。

2. IP 租用提供。当 DHCP 服务器收到 DHCPDISCOVER 数据包后，通过端口 68 给客户机回应一个 DHCPOFFER 信息，其中包含一个还没有被分配的有效 IP 地址。

3. IP 租用选择。客户机可能从不止一台 DHCP 服务器上收到 DHCPOFFER 信息。客户机选择 (3) 达到 DHCPOFFER，并发送 DHCPREQUEST 消息包。

4. IP 租用确认。DHCP 服务器向客户机发送一个确认(DHCPACK)信息，信息中包括 IP 地址、子网掩码、默认网关、DNS 服务器地址，以及 IP 地址的 (4) 。

【问题 2】(每空 1 分，共 6 分)

请在(5)～(10)空白处填写恰当的内容。

在 Linux 系统中使用__(5)__程序提供 DHCP 服务，DHCP 服务器启动时自动读它的配置文件__(6)__。DHCP 服务器配置文件如下所示。

```
ddns-update-style interim;
ignore client-updates;
default-lease-time 86400;
max-lease-time 129600;
subnet 192.168.0.0 netmask 255.255.255.0 {
option routers 192.168.0.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option domain-name-servers
61.233.1.1,  202.96.133.134;
Range 192.168.1.10 192.168.0.250;
}
```

根据这个文件中的内容，该 DHCP 服务的默认租期是__(7)__天，DHCP 客户机能获得的 IP 地址范围是从__(8)__到__(9)__；获得的 DNS 服务器 IP 地址为__(10)__。

【问题 3】(2 分)

在路由器上设置 DHCP__(11)__可以跨网段提供 DHCP 服务。

(11)备选答案：

A. 多个作用域　　B. 中继代理　　C. VPN

【问题 4】(每空 1 分，共 3 分)

请在(12)～(14)空白处填写恰当的内容。

Windows XP 用户在命令行方式下，通过__(12)__命令可以看到自己申请到的本机 IP 地址，用__(13)__可以重新向 DHCP 服务器申请 IP 地址，用__(14)__命令可以将 IP 地址释放。

4.3.4　同步练习参考答案

答案：

【问题 1】

(1) 0.0.0.0　(2) 255.255.255.255　(3) 第一个(或最先)　(4) 租约(或租期)

【问题 2】

(5) dhcpd　(6) /etc/dhcpd.conf　(7) 1(或一)　(8) 192.168.1.10

(9) 192.168.0.250　(10) 61.233.9.9 或 202.96.133.134 均正确

【问题 3】

(11) B

【问题 4】

(12) ipconfig 或 ipconfig/all　(13) ipconfig/renew　(14) ipconfig/release

4.4　代理服务器的配置

4.4.1　考点辅导

4.4.1.1　Internet 连接共享

ICS 是 Internet Connection Sharing 的缩写，是自 Windows 98 第二版以来，Windows 操作系统内置的一个多机共享上网组件。ICS 可以使多个用户利用一个 Internet 连接上网，非常适合在家庭网络环境中使用。ICS 需要两个连接才能工作：一个是外部连接，一般为 ADSL、Cable Modem 或 FTTx+LAN 的 Internet 连接；另一个是内部连接，用于把 ICS 主机连接到本地局域网中的其他计算机上。因此，充当主机的计算机至少需要两个网卡，一个用于外部连接，一个用于内部连接。

Internet 连接共享更适用于家庭网络或小型办公网络，其功能比较简单，设置也相当容易，不需要太多的专业知识就可以完成。通常在家庭网络环境下对安全的要求并不会太高，Internet 连接共享配合防火墙，就可以为局域网中的其他机器提供有效的保护。

下面以 Windows XP 为例，介绍如何配置 ICS，配置的过程分为配置 ICS 主机和客户机两部分，步骤如下。

1. ICS 主机端

(1)　在 ICS 主机上，首先打开“控制面板”窗口，如图 4-93 所示，单击“网络和 Internet 连接”图标，打开如图 4-94 所示的“网络和 Internet 连接”窗口。

图 4-93　“控制面板”窗口

图 4-94　“网络和 Internet 连接”窗口

(2)　单击“网络安装向导”图标，打开“网络安装向导”对话框，如图 4-95 所示。单击“下一步”按钮，打开如图 4-96 所示的“继续之前”界面，向导提醒用户检查网卡、Modem、电缆以及其他一些设备的状态。

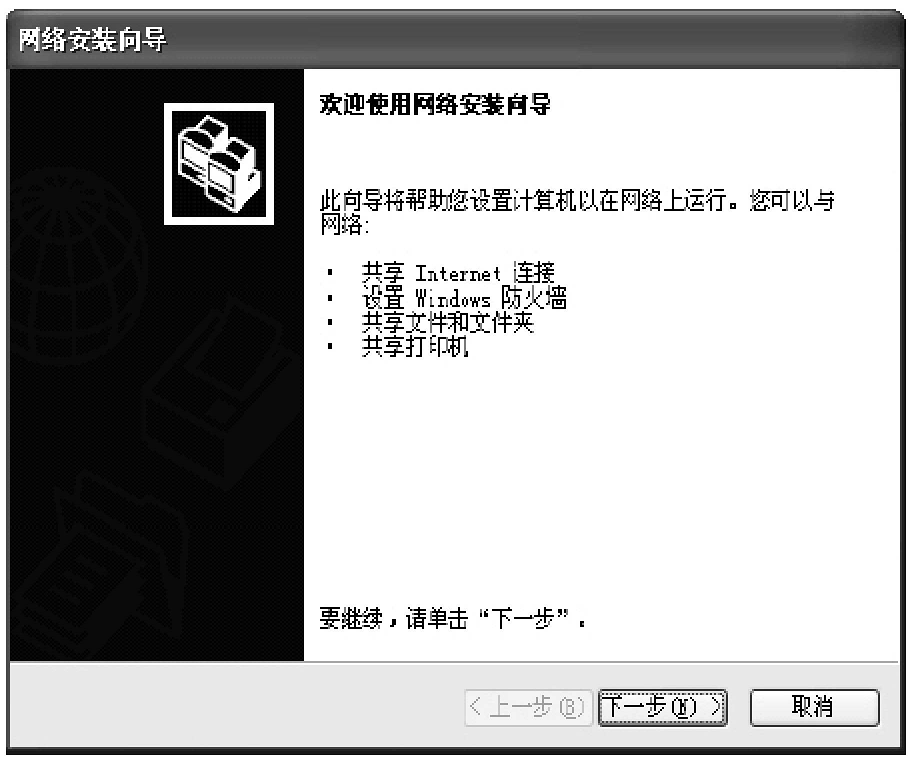


图 4-95　“网络安装向导”对话框

图 4-96　“继续之前”界面

(3) 单击“下一步”按钮，在如图 4-97 所示的“选择连接方法”界面中选中“这台计算机直接连接到 Internet。我的网络上的其他计算机通过这台计算机连接到 Internet”单选按钮。

(4) 单击“下一步”按钮，向导将列出 ICS 上主机所有的网络连接。选择与 Internet 相连的那个网络连接，如图 4-98 中的 WAN。

图 4-97　“选择连接方法”界面

图 4-98　选择 Internet 连接

(5) 单击“下一步”按钮，在如图 4-99 所示的“给这台计算机提供描述和名称”界面中输入 ICS 主机的计算机描述和计算机名。

(6) 单击“下一步”按钮，在打开的“命名您的网络”界面中输入一个工作组名称，如图 4-100 所示。

图 4-99　“给这台计算机提供描述和名称”界面

图 4-100　“命名您的网络”界面

(7)　单击“下一步”按钮，安装向导提示是否启用文件和打印机共享，以配置 Windows XP 防火墙，这里可根据实际需要选择启用还是关闭，如图 4-101 所示。

(8)　单击“下一步”按钮，向导列出前面各步骤中收集的设置信息，供用户在配置前做最后的确认，如图 4-102 所示。

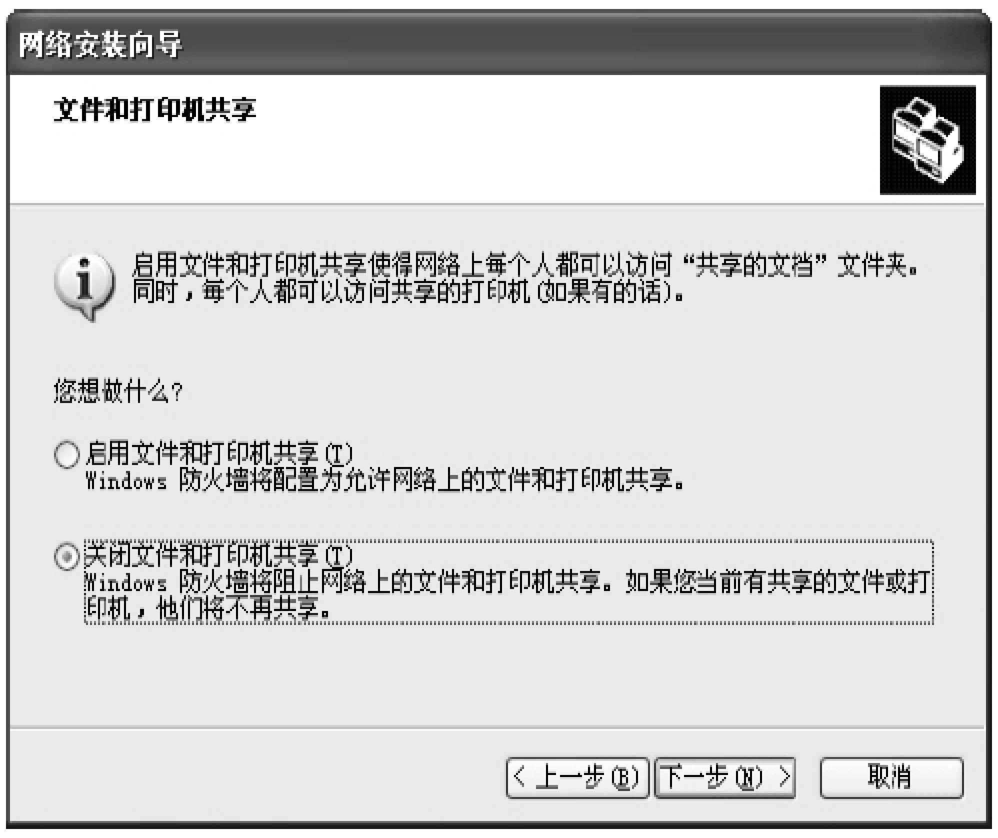


图 4-101　“文件和打印机共享”界面

图 4-102　“准备应用网络设置”界面

(9)　单击“下一步”按钮，向导开始设置网络。经过一段时间后，弹出如图 4-103 所示的“快完成了”界面，提示用户需要在网络中的每台计算机上运行一次网络安装向导。由于网络安装向导只在 Windows XP 中提供，如果要在没有运行 Windows XP 的计算机上运行该向导，则要使用 Windows XP 安装光盘或创建网络安装磁盘，这里我们选中“使用 Windows XP CD”单选按钮。

(10) 单击“下一步”按钮，向导给出在其他要联网的计算机上使用 Windows XP CD 运行网络安装向导的方法，即插入 CD，在出现的 CD 菜单上单击“执行其他任务”命令，再单击“安装家庭或小型办公网络”命令，按照系统提示操作即可，如图 4-104 所示。

图 4-103　“快完成了”界面

图 4-104　“要用 Windows XP CD 来运行向导”界面

(11) 单击“下一步”按钮，在如图 4-105 所示的“正在完成网络安装向导”界面中单击“完成”按钮，并重启计算机。

2. 客户机端

在客户机上按照上面所描述的步骤运行网络安装向导，但要在“选择连接方法”界面中选中“此计算机通过居民区的网关或网络上的其他计算机连接到 Internet”单选按钮，如图 4-106 所示。然后按照系统的提示一步一步完成整个安装过程。

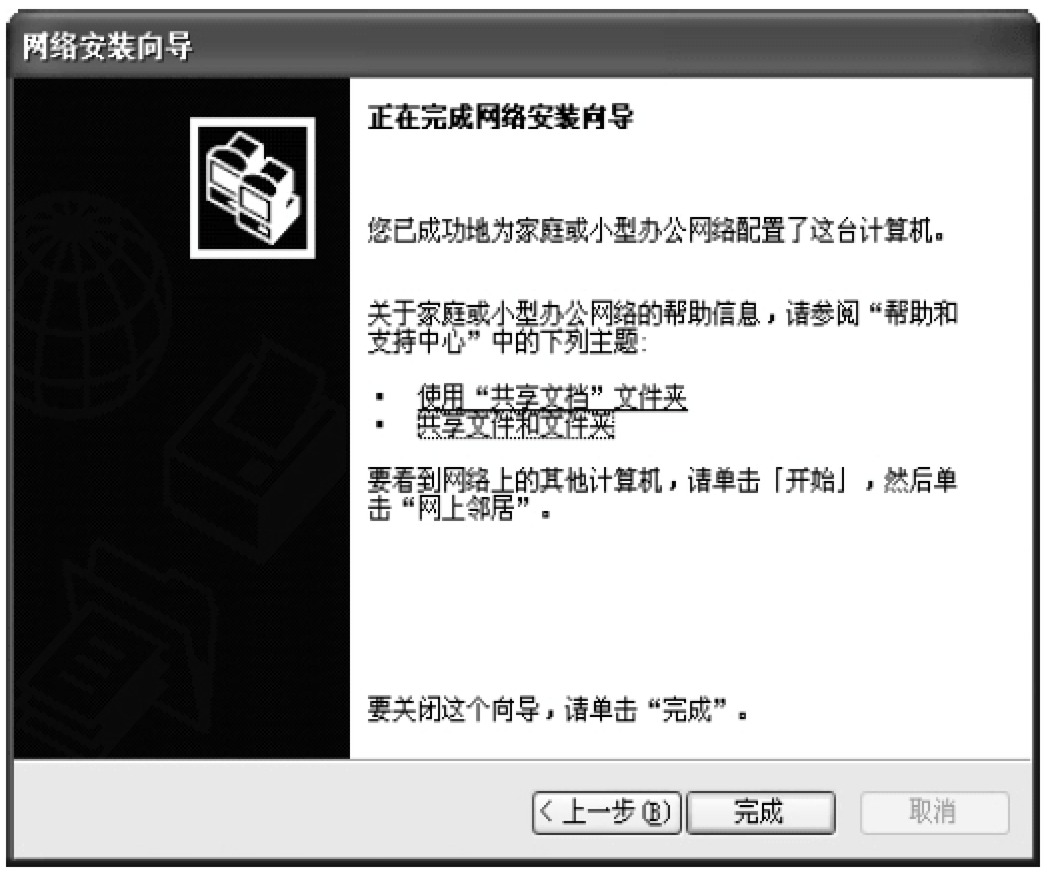


图 4-105 “正在完成网络安装向导”界面

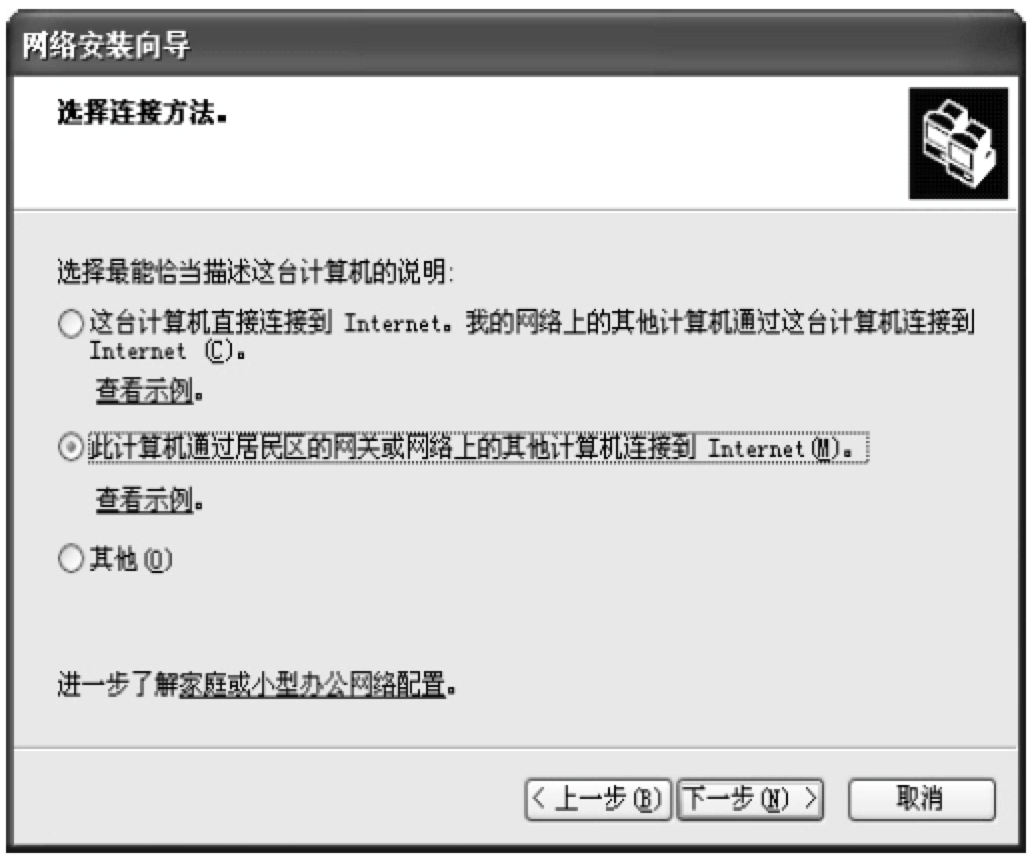


图 4-106 “选择连接方法”界面

另一种较为简便的设置 ICS 的方法是：在 ICS 主机上，打开与 Internet 连接的网卡的网络连接属性对话框，再切换到“高级”选项卡，如图 4-107 所示，选中“允许其他网络用户通过此计算机的 Internet 连接来连接”复选框，单击“确定”按钮，然后按照系统提示完成操作。此时该 ICS 主机与局域网相连的网卡的 IP 地址和子网掩码被自动设置为 192.168.0.1 和 255.255.255.0，如图 4-108 所示。而网络中的其他客户机只需将网卡的 TCP/IP 协议设为“自动获得 IP 地址”，即可共享 ICS 主机的 Internet 连接。

图 4-107 “高级”选项卡

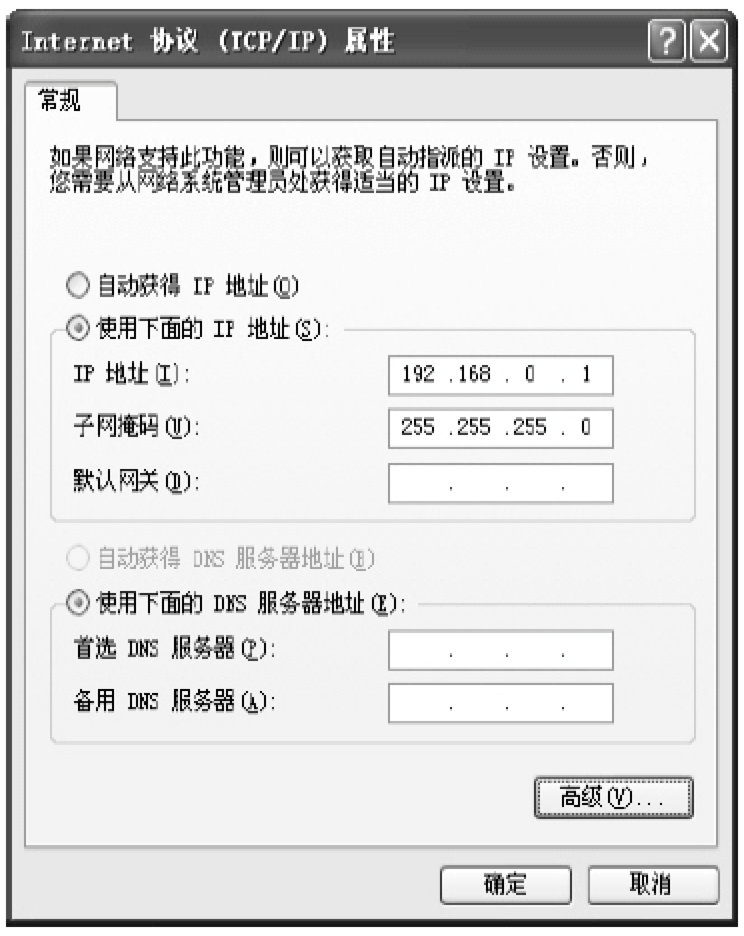


图 4-108 “Internet 协议(TCP/IP)属性”对话框

4.4.1.2 网络地址转换

NAT 的全称是 Network Address Translation，它通过一种把内部私有 IP 地址翻译成合法的正式网络 IP 地址技术，允许整体机构以一个公用 IP 地址出现在 Internet 上。

NAT 的工作原理如图 4-109 所示。

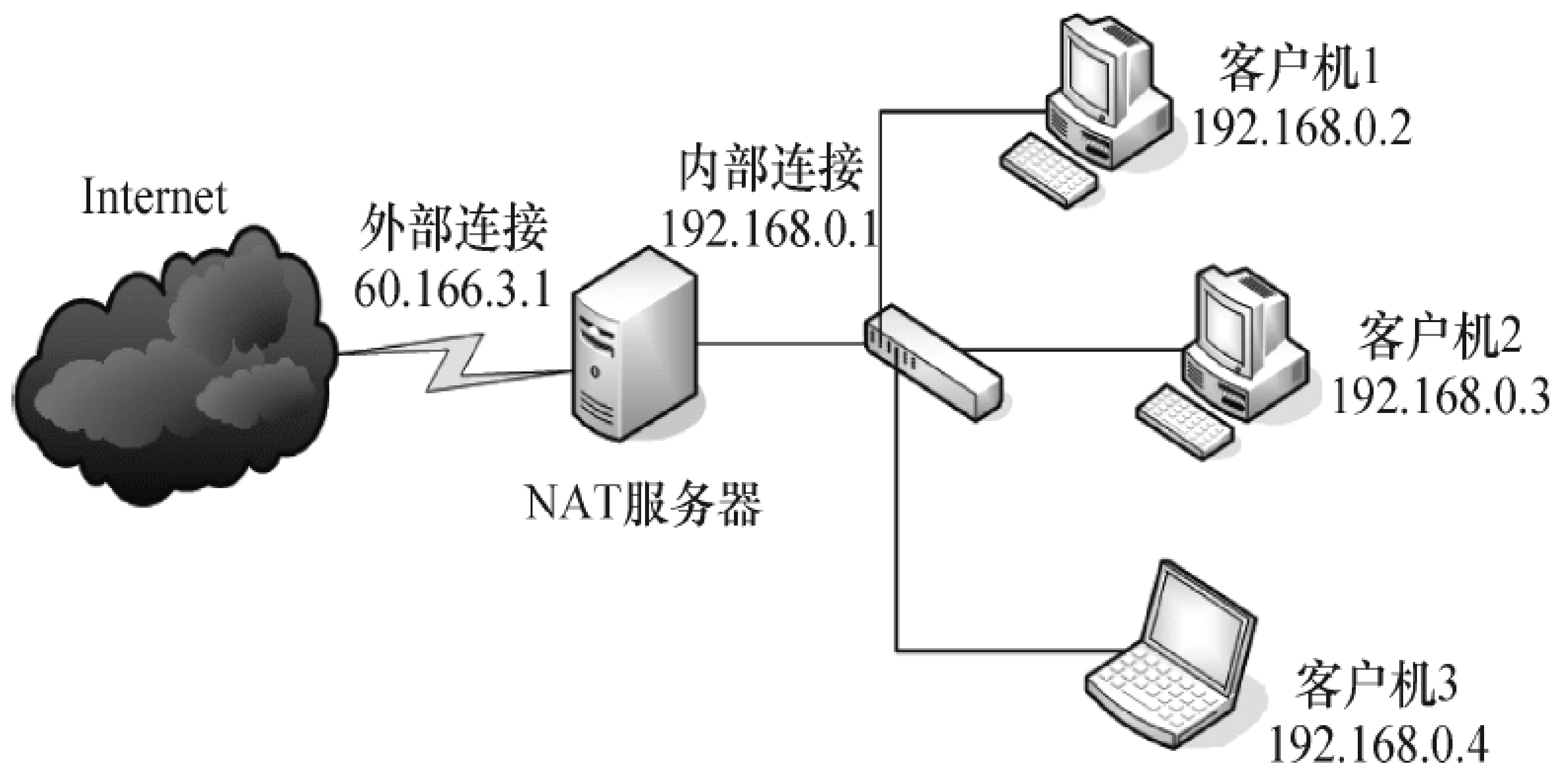


图 4-109　NAT 工作原理

从图 4-109 中可以看出，采用 NAT 共享 Internet 连接时，各主机在局域网内部通信时，使用内部私有 IP 地址，而当内部主机要和外部网络进行通信时，就由 NAT 服务器将内部私有 IP 地址转换成公用 IP 地址。此时内部网络对于外部网络来说是不可见的，而且内部计算机用户也意识不到 NAT 服务器的存在。NAT 技术很好地解决了公共 IP 地址紧缺的问题，但也存在一些缺点，满足不了一些网络应用的要求。

NAT 有三种类型：静态 NAT(Static NAT)、动态地址 NAT(Pooled NAT)和地址复用 PAT(Port Address Translation)。

静态 NAT 设置起来最为简单，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。

动态地址 NAT 则只是转换 IP 地址，它为每一个内部的 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号。对于频繁的远程连接也可以采用动态 NAT。当连接上远程用户之后，动态地址 NAT 就会分配给它一个 IP 地址，用户断开时，这个 IP 地址就会被释放而留待以后使用。

地址复用 PAT 能使多个内部地址映射到同一个合法的 IP 地址上，所以也可称作“多对一”NAT。通过使用 PAT 可以让成百上千个私有 IP 地址节点使用一个合法的 IP 地址访问 Internet。PAT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。PAT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备指定的 TCP 端口号。当 NAT 服务器接收到外部网络返回的应答信息时，会根据地址中的 TCP 端口号判断将数据包转发到网络中发起该访问请求的主机。

下面介绍如何在 Windows Server 2003 中配置 NAT，具体步骤如下。

(1) 单击“开始”按钮，在“管理工具”中选择“路由和远程访问”命令，打开如图 4-110 所示的“路由和远程访问”窗口。

(2) 在左窗格中右击服务器名，在弹出的快捷菜单中选择“配置并启用路由和远程访问”命令，如图 4-111 所示，打开安装向导，如图 4-1112 所示。

(3) 单击“下一步”按钮，在如图 4-113 所示的“配置”界面中，选中“网络地址转换”单选按钮。

(4) 单击“下一步”按钮，打开如图 4-114 所示的“NAT Internet 连接”界面，此处要为 NAT 选择一个 Internet 接口。若使用的是固定连接，则选中“使用此公共接口连接到

Internet”单选按钮，并在下面的列表中选中此连接。若使用的是拨号连接到 Internet，则选中“创建一个新的到 Internet 的请求拨号接口”单选按钮。这里我们选中“使用此公共接口连接到 Internet”单选按钮。

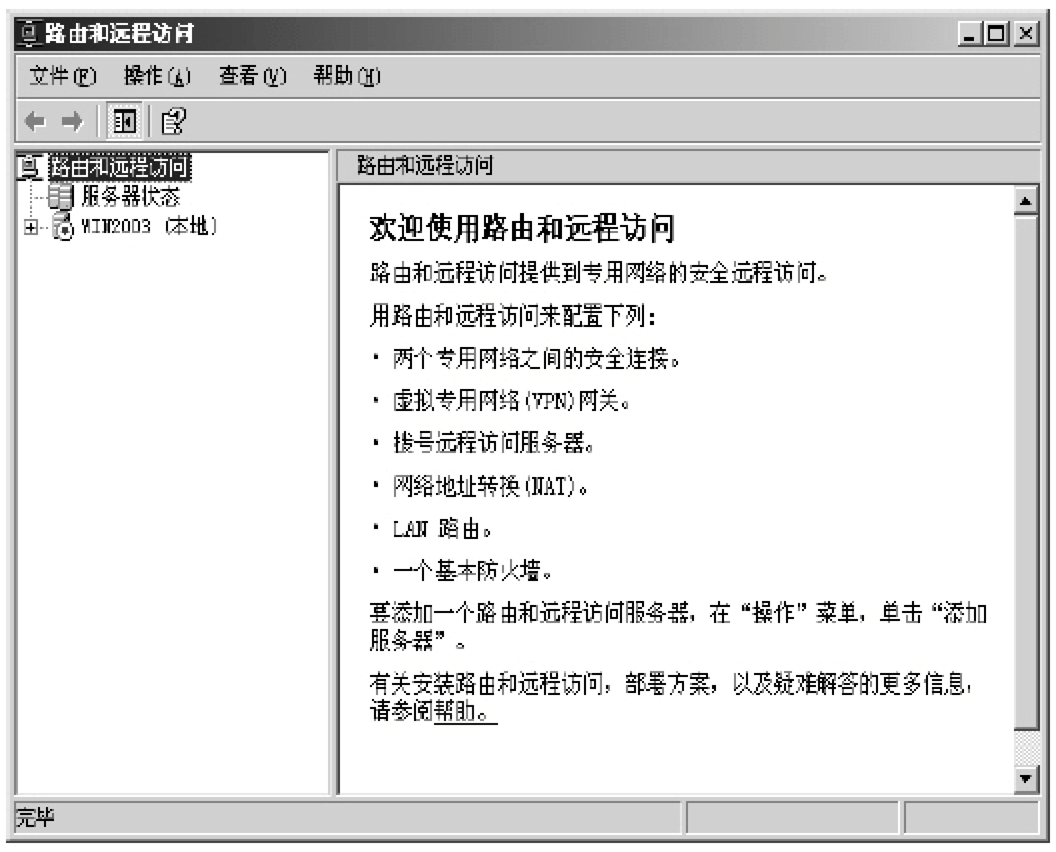


图 4-110 “路由和远程访问”窗口

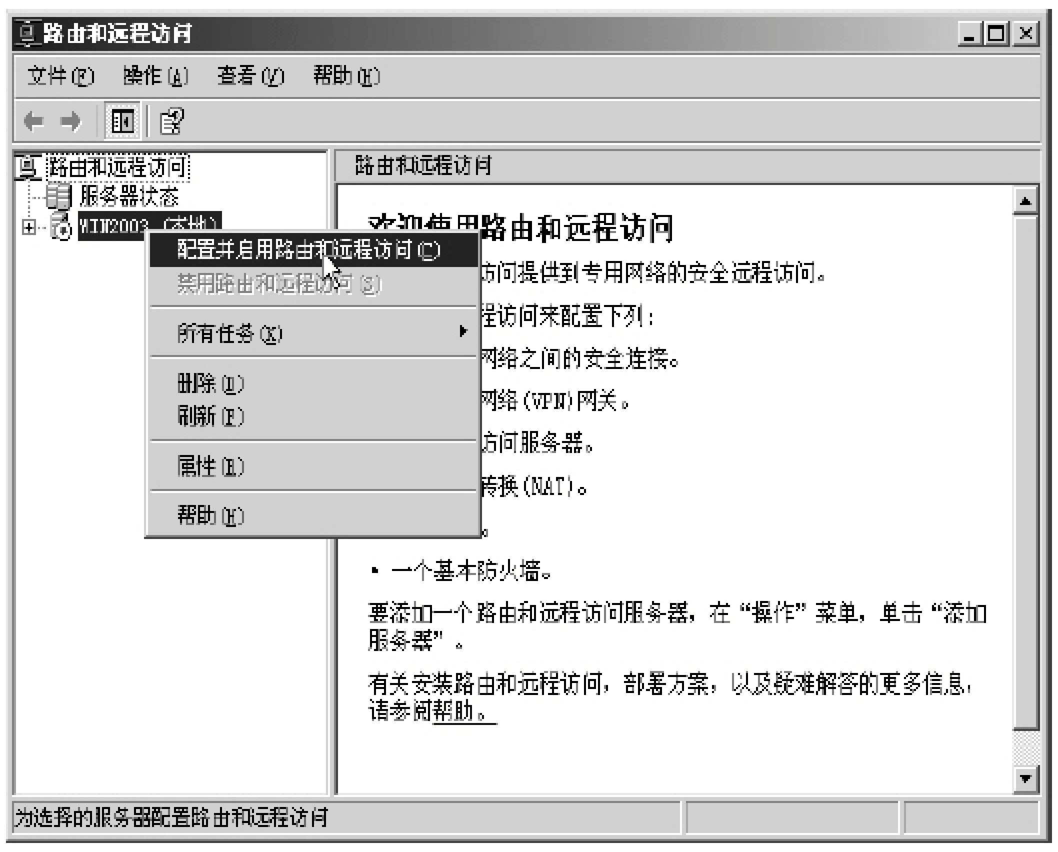


图 4-111 启动配置命令

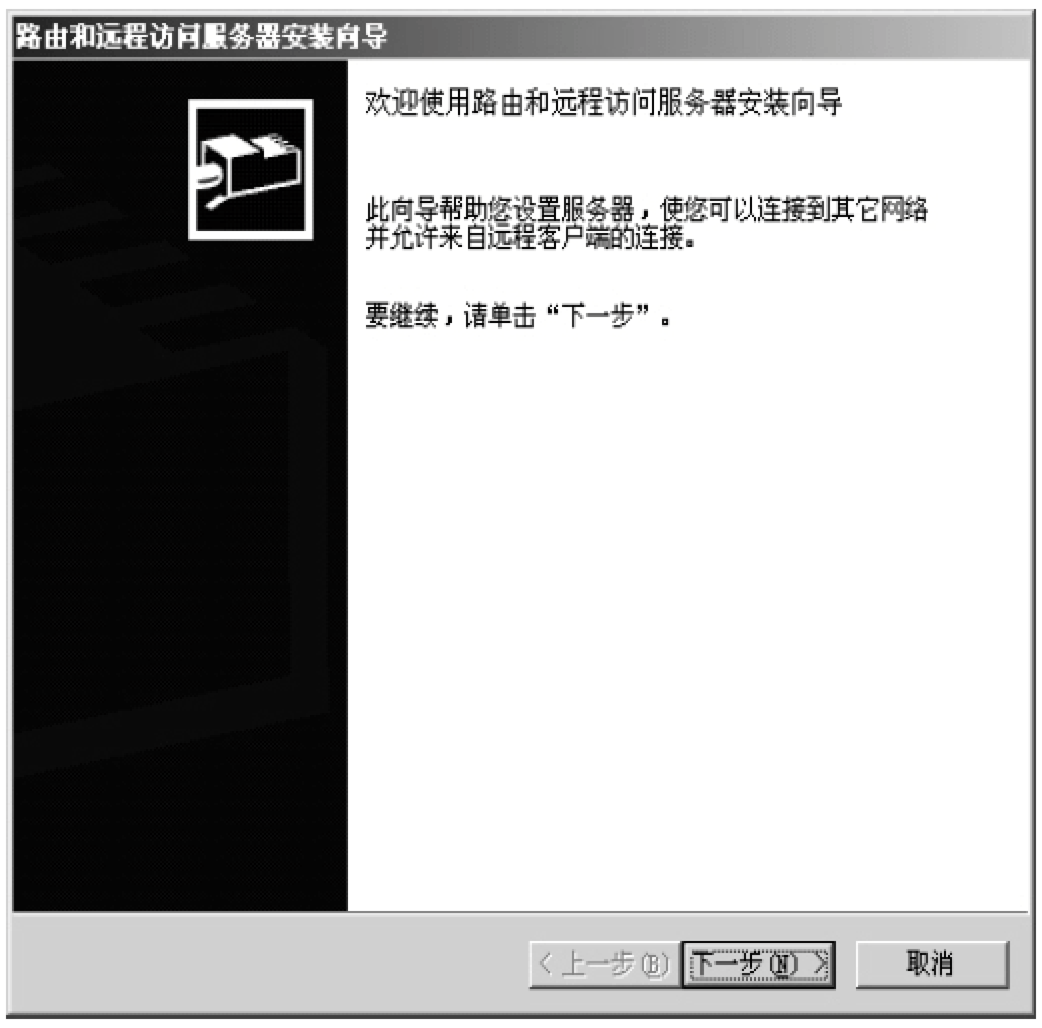


图 4-112 “路由和远程访问服务器安装向导”对话框

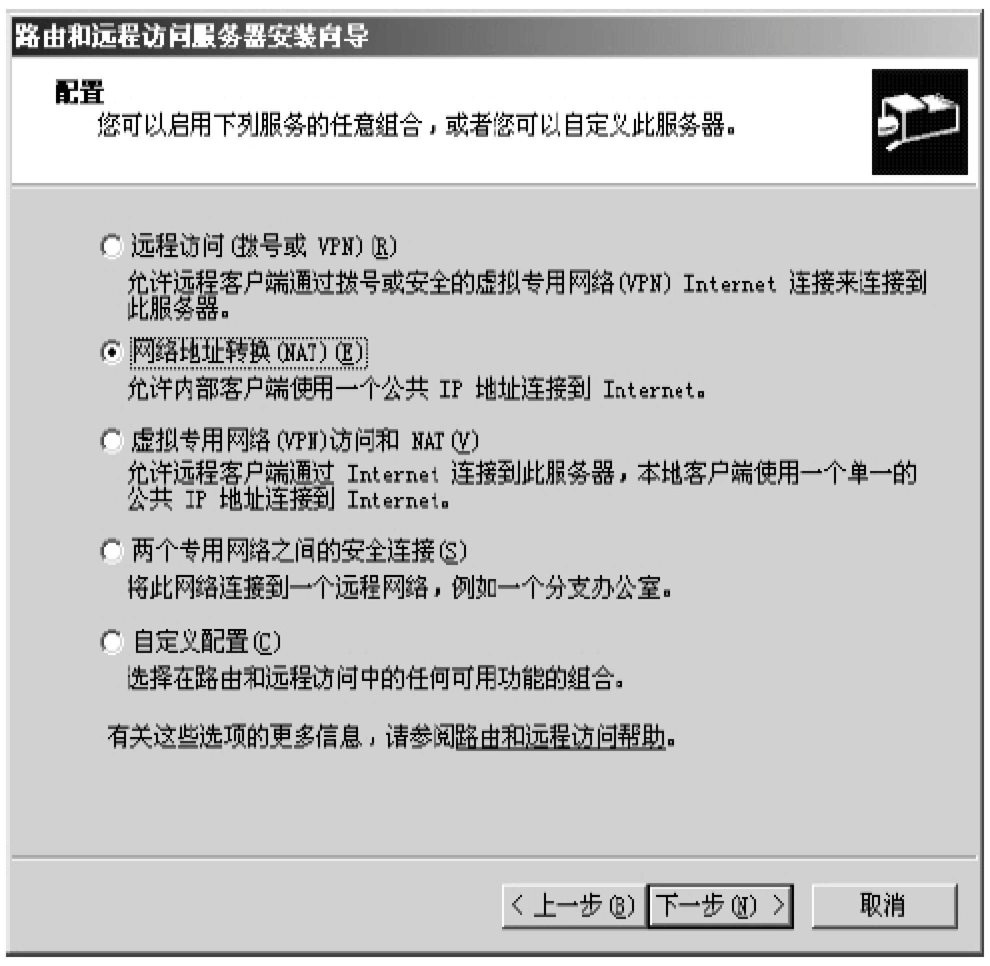


图 4-113 “配置”界面

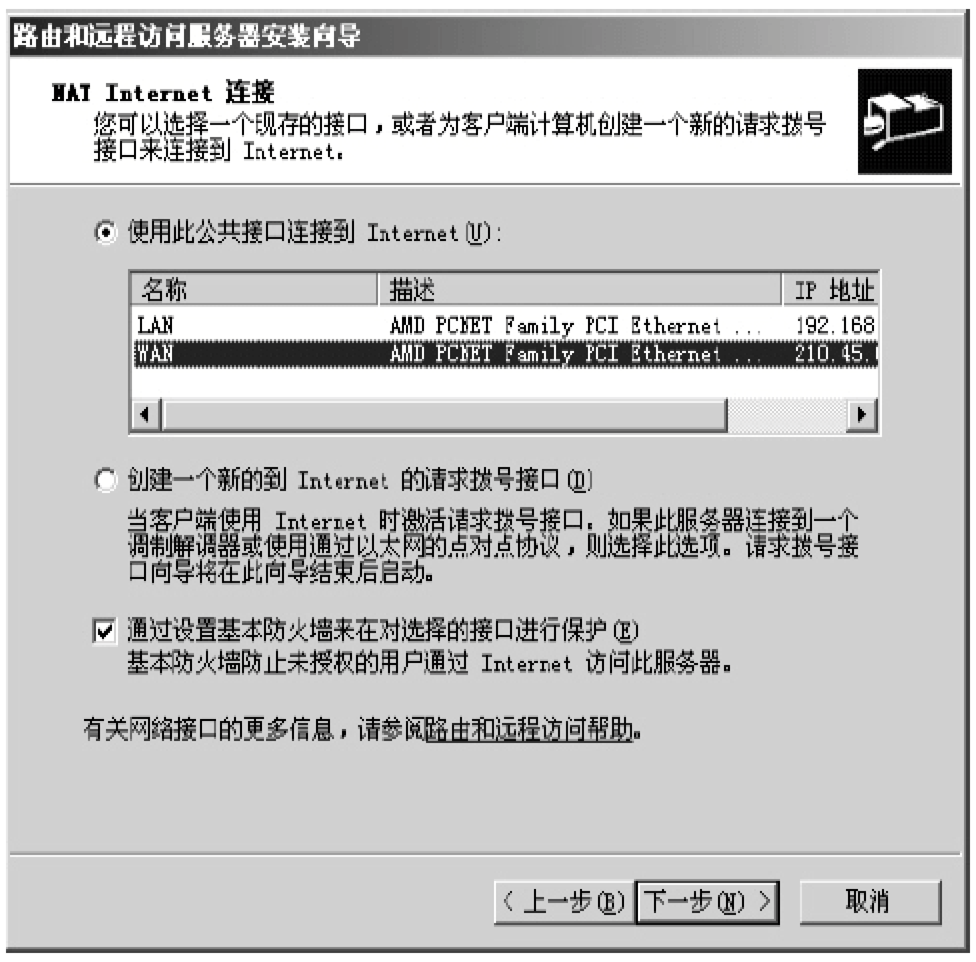


图 4-114 “NAT Internet 连接”界面

(5) 单击“下一步”按钮，在打开的如图 4-115 所示的界面中单击“完成”按钮，向导开始配置并启动路由和远程访问服务，配置后的控制台界面如图 4-116 所示。

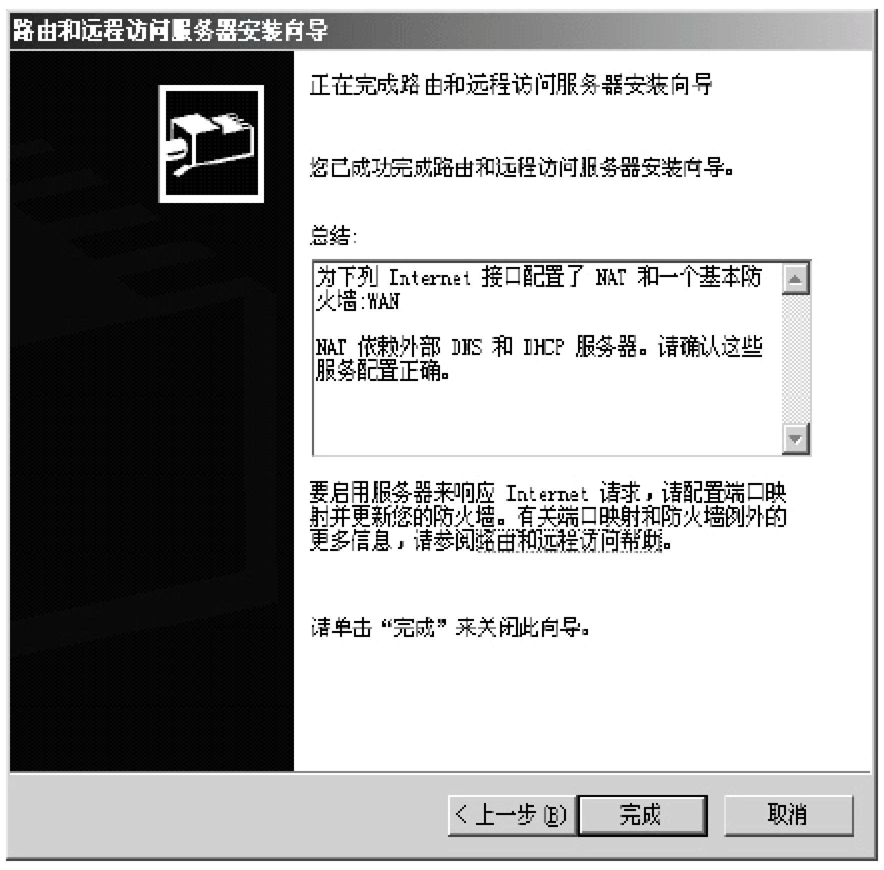


图 4-115　“正在完成路由和远程访问服务器安装向导”界面

图 4-116　配置 NAT 后的“路由和远程访问”控制台

4.4.2　典型例题分析

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】终端服务可以使客户远程操作服务器，在 Windows Server 2003 中开启终端服务时需要分别安装终端服务的服务器端和客户端，图 4-117 为客户机 Host1 连接终端服务器 Server1 的网络拓扑示意图。

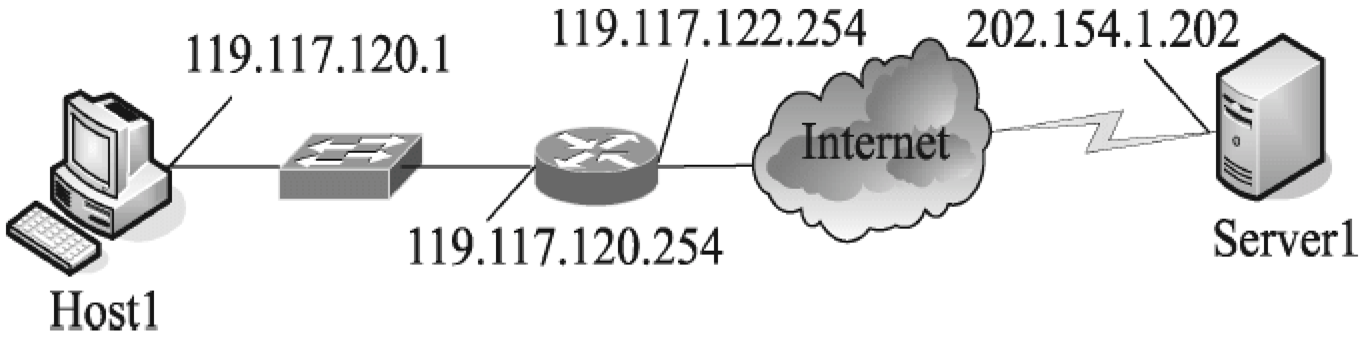


图 4-117　网络拓扑示意图

Host1 和 Server1 账户如表 4-2 所示。

表 4-2　Host1 和 Server1 账户

账 户 名	主　机	所 属 组
Admin1	Host1	Administrators
RDU1	Host1	Power Users
Admin2	Server1	Administrators
RDU2	Server1	Remote Desktop Users

图 4-118 是 Server1 系统属性的“远程”选项卡，图 4-119 是 Server1 RDP-Tcp 属性的“环境”选项卡，图 4-120 为 Host1 采用终端服务登录 Server1 的用户登录界面。

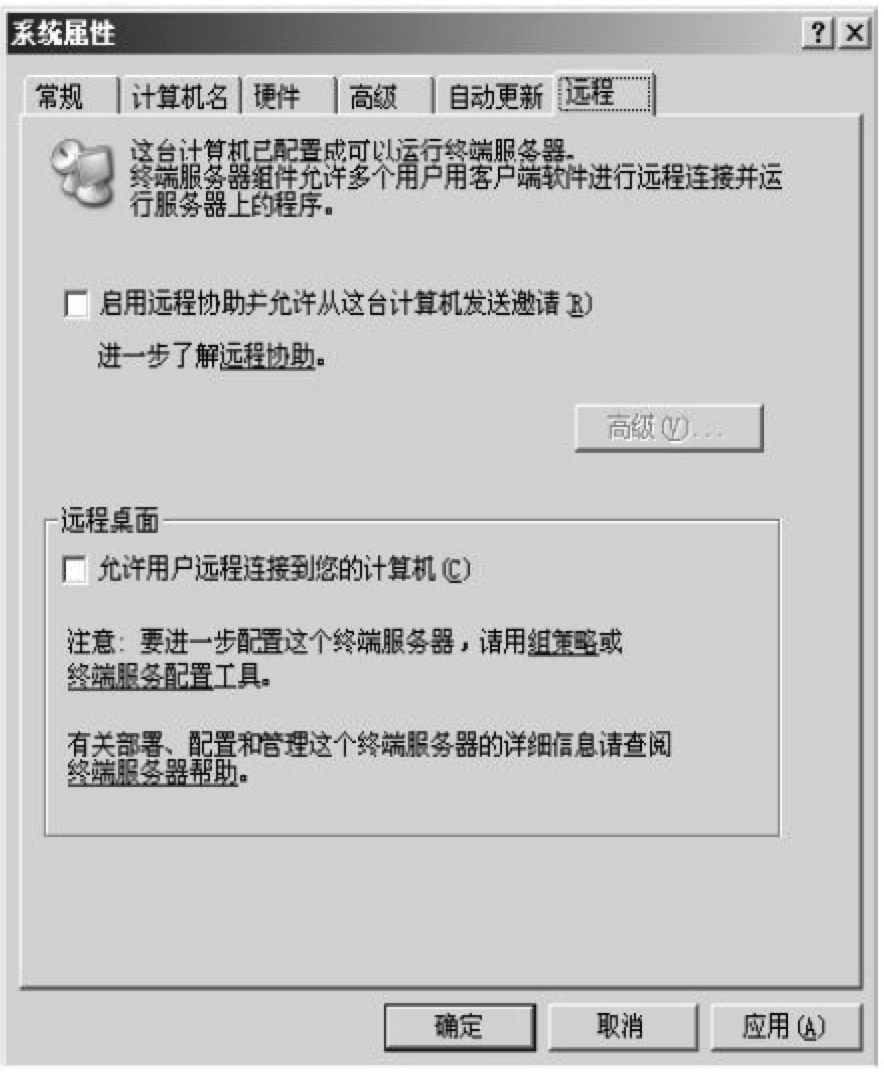


图 4-118 “远程”选项卡

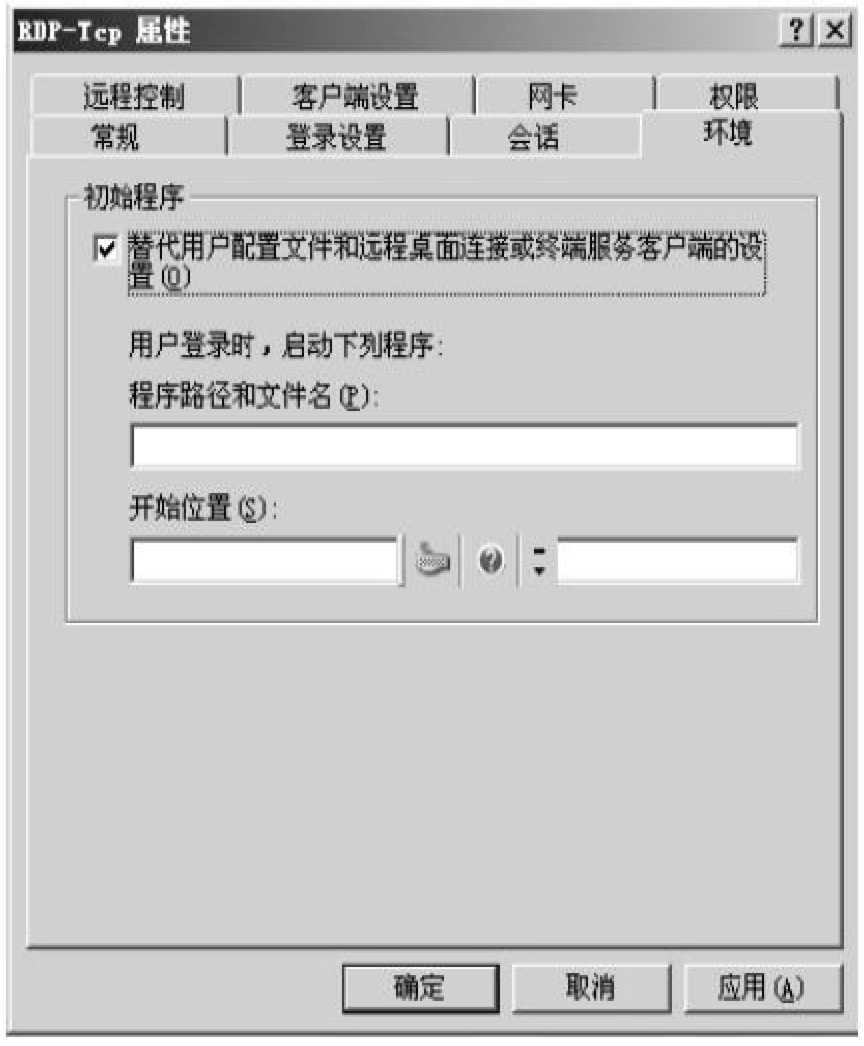


图 4-119 “环境”选项卡

此外，在 Server1 中为了通过日志了解每个用户的行踪，把“D:\tom\note.bat”设置成用户的登录脚本，通过脚本中的配置来记录日志。

【问题 1】(3 分)

默认情况下，RDU2 对终端服务具有__(1)__和__(2)__权限。

(1)、(2)备选答案：

A. 完全控制　　B. 用户访问　　C. 来宾访问　　D. 特别

【问题 2】(7 分)

将 RDU2 设置为 Server1 的终端服务用户后，在 Host1 中登录 Server1 时，图 4-120 中“计算机”文本框应填入__(3)__；“用户名”文本框应填入__(4)__。

此时发现 Host1 不能远程登录终端服务器，可能的原因是__(5)__。

图 4-120 登录设置

【问题 3】(2 分)

在图 4-119 "程序路径和文件名" 文本框中应输入__(6)__。

【问题 4】(3 分)

note.bat 脚本文件如下。

```
time /t>>note.log
netstat -n -p tcp|find":3389">>note.log
start Explorer
```

第一行代码用于记录用户登录的时间，"time /t"的意思是返回系统时间，使用符号">>"把这个时间记入 "note.log" 作为日志的时间字段。请解释下面命令的含义。

```
netstat -n -p tcp|find":3389">>note.log
```

答案：

【问题 1】

(1) B　(2) C

注意：(1)和(2)的答案可以互换。

【问题 2】

(3) 210.154.1.202　(4) RDU2

(5) 图 4-118 中没有选中 "允许用户远程连接到您的计算机" 复选框。

【问题 3】

(6) D:\tom\note.bat

【问题 4】 将通过 3389 端口访问主机的 TCP 协议状态信息写入 note.log 中，或将远程访问主机的信息记录在日志文件 note.log 中。

解析：

【问题 1】 RDU2 是远程桌面组的成员，只有访问权限而不具备完全控制权。

【问题 2】 要远程登录终端服务时，需要在 "计算机" 文本框中输入终端服务器的 IP 地址，Server1 为终端服务器，其地址为 210.154.1.202。在 "用户名" 文本框中输入账户名 "RDU2"。

此外，要登录远程服务器，服务器中必须允许用户远程连接。

【问题 3】 此处填入的是日志文件的存放目录。由题目可知，在 Server1 中把 "D:\tom\note.bat" 设置成用户的登录脚本，通过脚本中的配置来记录日志。

【问题 4】 netstat –n –p tcp | find":3389">>note.log 的目的是将远程访问主机的信息记录在日志文件 note.log 中，记录 3389 端口的 TCP 协议状态。

4.4.3　同步练习

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】 某公司的两个部门均采用 Windows 2003 的 NAT 功能共享宽带连接访问 Internet，其网络结构和相关参数如图 4-121 所示。ISP 为该公司分配的公网 IP 地址段为 202.117.12.32/29。

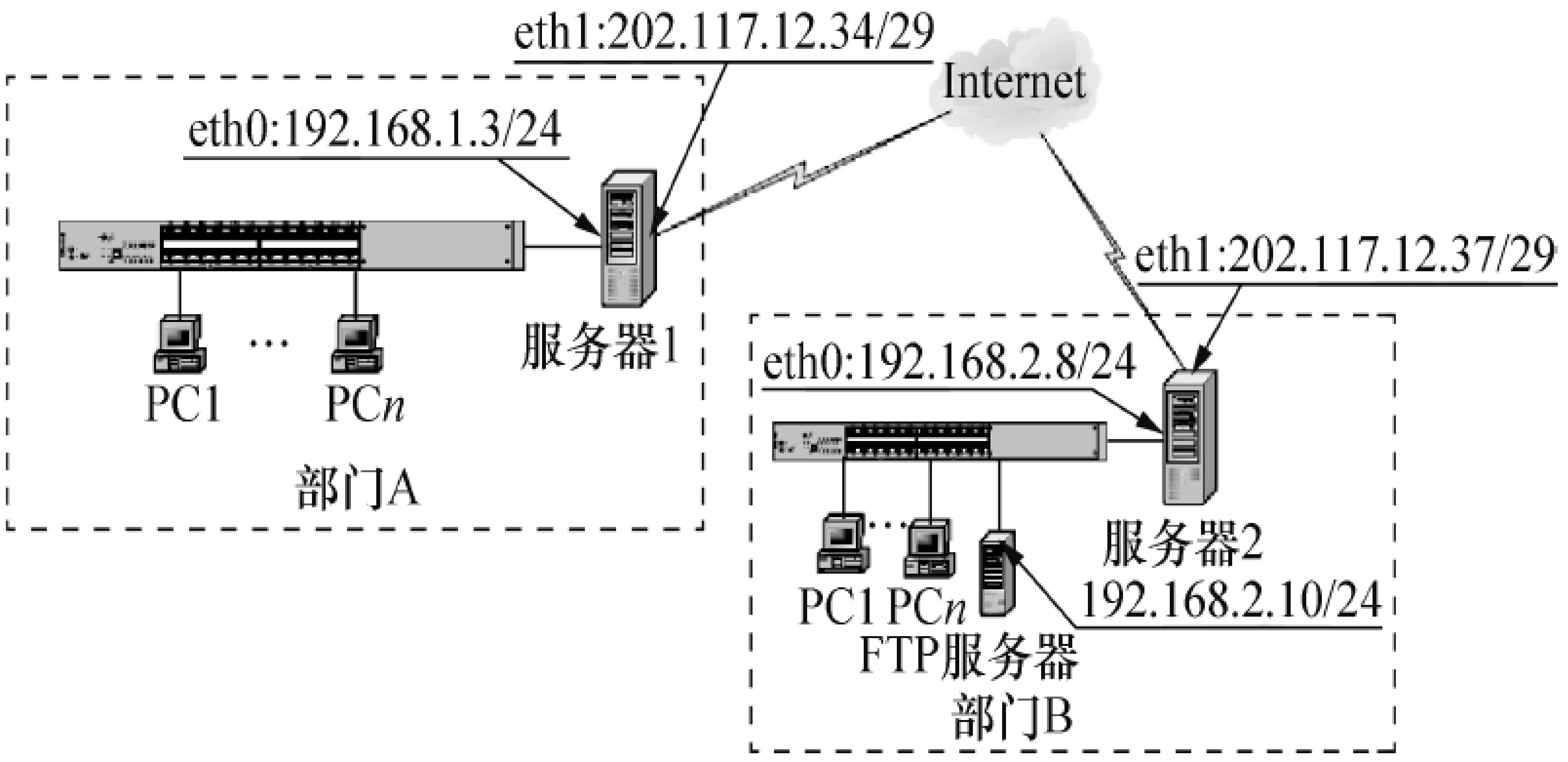


图 4-121　网络拓扑结构图

【问题 1】(2 分)

在 Windows 2003 中，__(1)__ 不能实现 NAT 功能。

(1)备选答案：

A. 终端服务管理器　　　B. Internet 连接共享　　　C. 路由和远程访问

【问题 2】(4 分)

在图 4-122 所示的窗口中，为部门 B 的服务器 2 配置“路由和远程访问”功能，新增 eth0 和 eth1 上的网络连接。eth0 上的网络连接应该选中图 4-123 中的__(2)__选项进行配置，eth1 上的网络连接应该选中图 4-123 中的__(3)__选项进行配置。

(2)、(3)备选答案：

A. 专用接口连接到专用网络

B. 公用接口连接到 Internet

C. 仅基本防火墙

【问题 3】(2 分)

部门 B 中主机 PC1 的默认网关地址应配置为__(4)__才能访问 Internet。

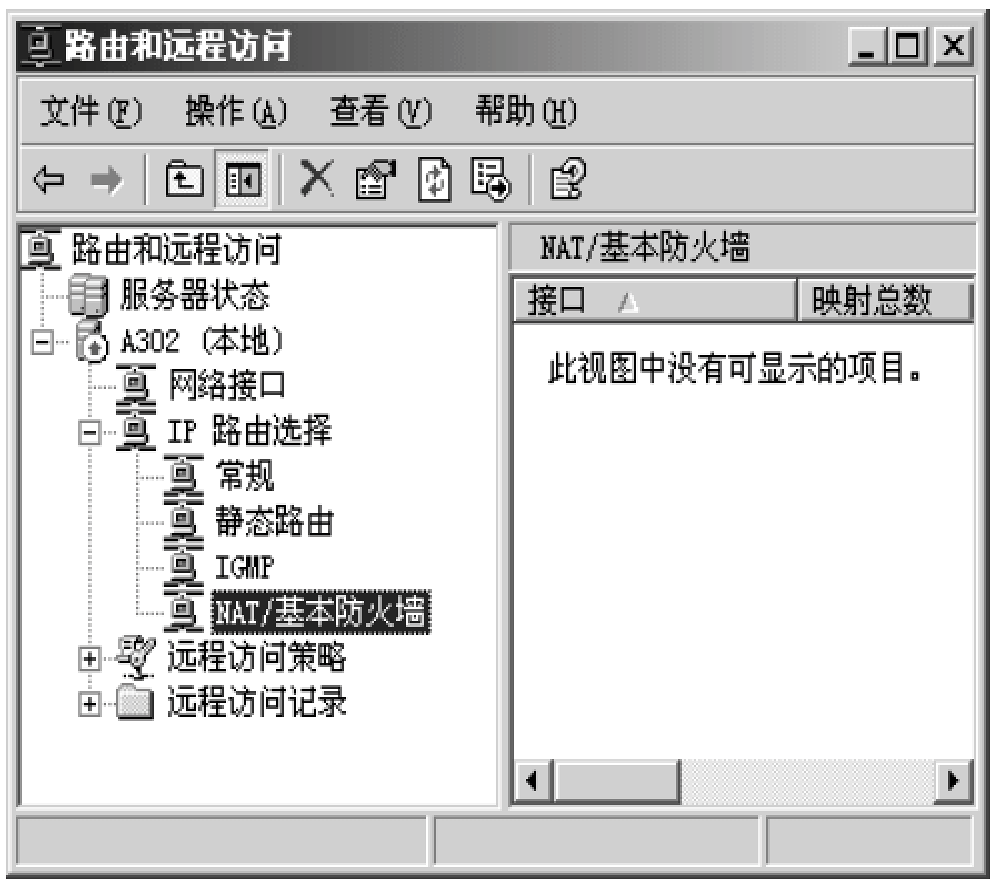


图 4-122　“路由和远程访问”窗口

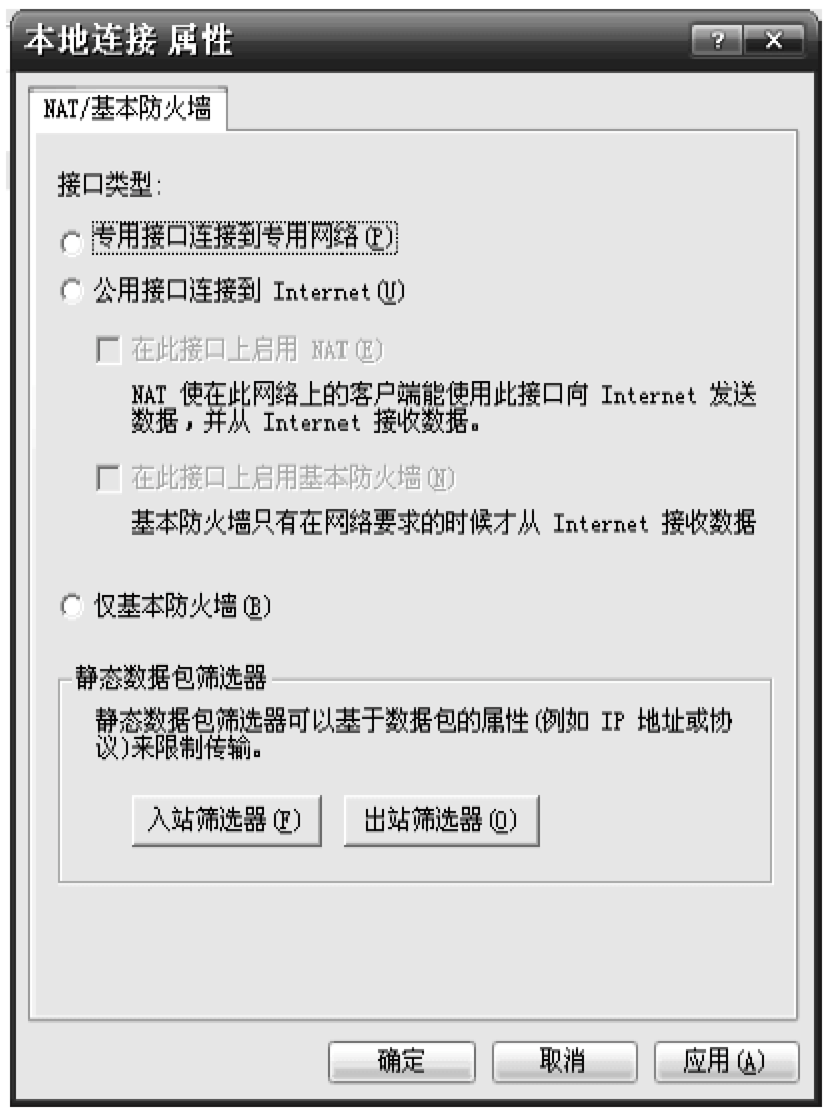


图 4-123　eth0 的网络连接

【问题 4】(2 分)

在部门 B 的服务器 2 中，如果将 ISP 分配的可用公网 IP 地址添加到地址池(如图 4-124 所示)，那么服务器 1 收到来自部门 B 的数据包的源地址可能是 (5) 。如果部门 B 中两台不同 PC 同时发往公网的两个数据包的源地址相同，则它们通过 (6) 相互区分。

【问题 5】(2 分)

在服务器 2 的 eth1 上启用基本防火墙，如果希望将 202.117.12.38 固定分配给 IP 地址为 192.168.2.10 的 FTP 服务器，且使得公网中主机可以访问部门 B 中的 FTP 服务，应该在图 4-124 和图 4-125 所示的对话框中如何配置？

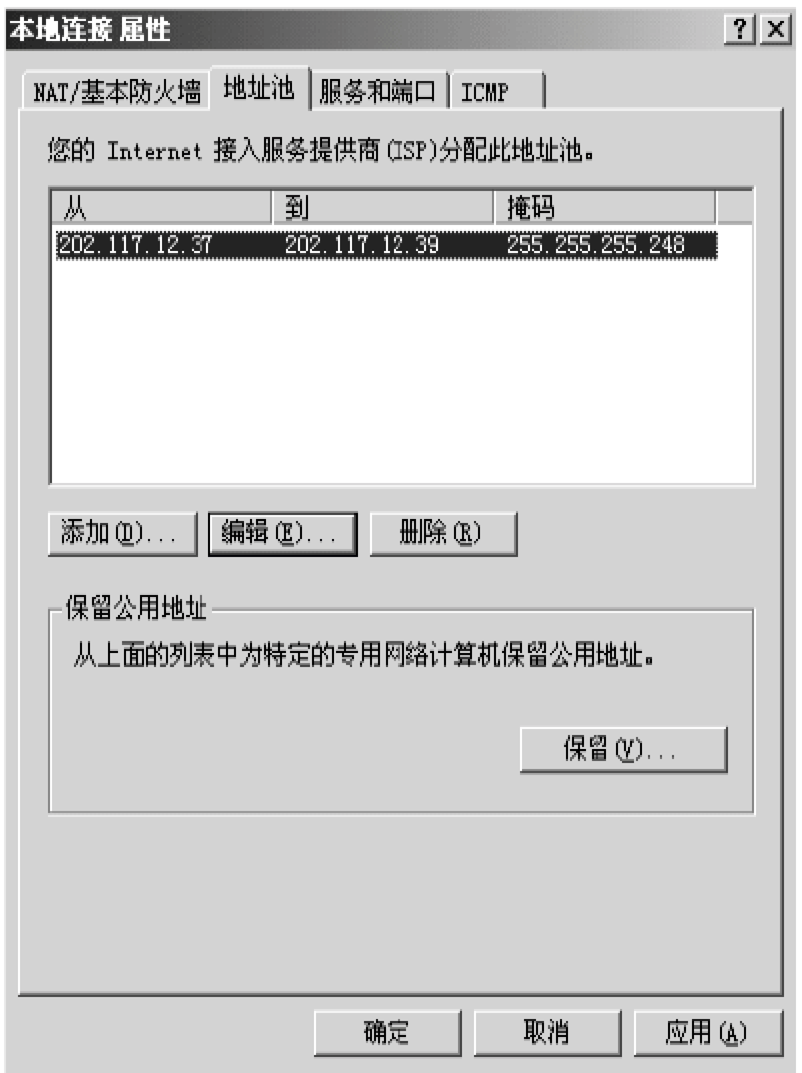


图 4-124　“地址池”选项卡

图 4-125　“添加保留区”对话框

【问题 6】(3 分)

为了实现部门 A 和部门 B 中的主机互相通信，在服务器 1 和服务器 2 上都运行了“路由和远程访问”服务，两台服务器的静态路由信息应配置如表 4-3 所示。

表 4-3　路由信息配置表

主　机	接　口	目　标	网络掩码	网　关	跃 点 数
服务器 1	WAN 连接	(7)	(8)	(9)	1
服务器 2	WAN 连接	(10)	(11)	(12)	1

4.4.4　同步练习参考答案

答案：

【问题 1】

(1) A 或终端服务管理器

【问题 2】

(2) A 或专用接口连接到专用网络　　　(3) B 或公用接口连接到 Internet

【问题 3】

(4) 192.168.2.8

【问题 4】

(5) 202.117.12.37 或 202.117.12.38

(6) 端口号

【问题 5】

在“本地连接 属性”对话框中单击“保留”按钮，在弹出的对话框中单击“添加”按钮，出现“添加保留区”对话框，依次填入 IP 地址 202.117.12.38 和 192.168.1.3，选中“允许将会话传入到此地址”复选框，单击“确定”按钮。然后在“本地连接 属性”对话框的“服务和端口”选项卡中选中“FTP 服务”即可。

【问题 6】

(7) 192.168.2.0　　(8) 255.255.255.0　　(9) 202.117.12.37

(10) 192.168.1.0　　(11) 255.255.255.0　　(12) 202.117.12.34

4.5 本章小结

本章知识点在 2014 年的新大纲中变化不大，只是要求更加明细化，并添加了网络安全的内容。

本章主要要求考生掌握 Windows 网络服务的基本功能以及在 Windows 平台下相关服务器的配置。主要内容包括 IIS 服务器的配置、DNS 服务器的配置、DHCP 服务器的配置和代理服务器的配置。

本章内容为下午科目的重点内容，为每次考试必考的内容。本章的每小节中都组织了大量的针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点，有助于考生巩固所掌握的知识。

第 5 章　Linux 应用服务器的配置

大纲要求：

- ◆ DHCP 服务器的原理和配置(Linux)。
- ◆ DNS，包括 URL、域名解析和 DNS 服务器的配置(Linux)。
- ◆ 电子邮件服务器配置(Linux)。
- ◆ WWW，包括虚拟主机、WWW 服务器配置(Linux)和 WWW 服务器的安全配置。
- ◆ FTP 服务器，包括 FTP 服务器的访问和 FTP 服务器的配置(Linux)。

5.1　Apache 服务器的配置

5.1.1　考点辅导

5.1.1.1　主站点的配置

Apache 是使用排名世界第一的 Web 服务器软件，它可以运行在几乎所有广泛使用的计算机平台上。

Apache 源于 NCSA HTTPd 服务器，经过多次修改，成为世界上最流行的 Web 服务器软件之一。Apache 取自“a patchy server”的读音，意思是充满补丁的服务器。因为它是自由软件，所以不断有人来为它开发新的功能、新的特性，并修改原来的缺陷。Apache 的特点是简单、速度快、性能稳定，并可作为代理服务器来使用。

Apache 的配置由 httpd.conf 文件完成，因此下面的配置指令都是在 httpd.conf 文件中修改。

1. 基本配置

ServerRoot“/mnt/software/apache2”# apache 表示软件安装的位置。其他指定的目录如果没有指定绝对路径，则表示相对于该目录。“#”后的内容表示对语句的解释。

```
PidFile logs/httpd.pid #第一个 httpd 进程(所有其他进程的父进程)的进程号文件位置
Listen 80 #服务器监听的端口号
ServerName www.clusting.com:80 #主站点名称(网站的主机名)
ServerAdmin admin@clusting.com #管理员的邮件地址
DocumentRoot "/mnt/web/clusting" #主站点的网页存储位置
```

以下是对主站点的目录进行访问控制。

```
<Directory "/mnt/web/clusting">
Options FollowSymLinks
AllowOverride None
Order allow,deny
```

```
Allow from all
</Directory>
```

在上面这段目录属性配置中，主要有以下选项。

(1) Options：配置特定目录使用的相关特性，常用的值和基本含义如下。

- ExecCGI：在该目录下允许执行 CGI 脚本。
- FollowSymLinks：在该目录下允许文件系统使用符号连接。
- Indexes：当用户访问该目录时，如果用户找不到 DirectoryIndex 指定的主页文件(如 index.html)，则返回该目录下的文件列表给用户。
- SymLinksIfOwnerMatch：当使用符号连接时，只有当符号连接的文件拥有者与实际文件的拥有者相同时才可以访问。

(2) AllowOverride：允许可存在于.htaccess 文件中的指令类型(.htaccess 文件名是可以改变的，其文件名由 AccessFileName 指令决定)。

- None：不搜索该目录下的.htaccess 文件(可以减小服务器开销)。
- All：在.htaccess 文件中可以使用所有的指令。

(3) Order：控制在访问时 allow 和 deny 两个访问规则哪个优先。

- allow：允许访问的主机列表(可用域名或子网，如 Allow from 192.168.0.0/16)。
- deny：拒绝访问的主机列表。

以下是对首页文件的格式进行设置。

```
DirectoryIndex index.html index.htm index.php #主页文件的设置(将主页文件设置为
index.html，index.htm 和 index.php)
```

2. 服务器的优化

Apache 主要的优势就是对多处理器的支持更好，在编译时通过使用 with-mpm 选项来决定 Apache 的工作模式。如果知道当前的 Apache 使用什么工作机制，可以通过 httpd -l 命令列出 Apache 的所有模块，就可以知道其工作方式。

(1) prefork：如果 httpd -l 列出 prefork.c，则需要对下面的段进行配置。

```
<IfModule prefork.c>
StartServers 5 #启动 Apache 时启动的 httpd 进程个数
MinSpareServers 5 #服务器保持的最小空闲进程数
MaxSpareServers 10 #服务器保持的最大空闲进程数
MaxClients 150 #最大并发连接数
MaxRequestsPerChild 1000 #每个子进程被请求服务多少次后被 kill 掉。0 表示不限制，推
荐设置为 1000
</IfModule>
```

在该工作模式下，服务器启动后启动 5 个 httpd 进程(连同父进程共 6 个，通过 ps -ax|grep httpd 命令可以看到)。当有用户连接时，Apache 会使用一个空闲进程为该连接服务，同时父进程会复制一个子进程，直到内存中的空闲进程达到 MaxSpareServers 为止。采用该模式可以兼容一些旧版本的程序，是默认编译时的选项。

(2) worker：如果 httpd -l 列出 worker.c，则需要对下面的段进行配置。

```
<IfModule worker.c>
```

```
StartServers 2 #启动 Apache 时启动的 httpd 进程个数
MaxClients 150 #最大并发连接数
MinSpareThreads 25 #服务器保持的最小空闲线程数
MaxSpareThreads 75 #服务器保持的最大空闲线程数
ThreadsPerChild 25 #每个子进程产生的线程数
MaxRequestsPerChild 0 #每个子进程被请求服务多少次后被 kill 掉。0 表示不限制，推荐设
置为 1000
</IfModule>
```

采用该模式可以用线程来监听客户的连接。当有新客户连接时，由其中的一个空闲线程接受连接。服务器在启动时启动两个进程，每个进程产生的线程数是固定的(由 ThreadsPerChild 决定)，因此启动时有 50 个线程。当 50 个线程不够用时，服务器自动 fork 一个进程，再产生 25 个线程。

(3) perchild：如果 httpd -l 列出 perchild.c，则需要对下面的段进行配置。

```
<IfModule perchild.c>
NumServers 5 #服务器启动时启动的子进程数
StartThreads 5 #每个子进程启动时启动的线程数
MinSpareThreads 5 #内存中的最小空闲线程数
MaxSpareThreads 10 #最大空闲线程数
MaxThreadsPerChild 2000 #每个线程最多被请求多少次后退出。0 表示不限制
MaxRequestsPerChild 10000 #每个子进程服务多少次后被重新 fork。0 表示不限制
</IfModule>
```

该模式下，子进程的数量是固定的，线程数不受限制。当客户端连接到服务器时，由空闲的线程提供服务。如果空闲线程数不够，子进程会自动产生线程来为新的连接服务。该模式用于多站点服务器。

3. HTTP 返回信息配置

(1) ServerTokens Prod #该参数设置 HTTP 头部返回的 Apache 版本信息，可用的值和含义如下。

- Prod：仅软件名称，如 Apache。
- Major：包括主版本号，如 Apache/2。
- Minor：包括次版本号，如 Apache/2.0。
- Min：仅 Apache 的完整版本号，如 Apache/2.0.54。
- OS：包括操作系统类型，如 Apache/2.0.54(UNIX)。
- Full：包括 Apache 支持的模块及模块版本号，如 Apache/2.0.54 (UNIX) mod_ssl/2.0.54 OpenSSL/0.9.7g。

(2) ServerSignature Off# 该参数可以设置在页面产生错误时是否出现服务器版本信息，On 为显示，Off 为不显示，推荐设置为 Off。

4. 持久性连接设置

KeepAlive On #开启持久性连接功能，即当客户端连接到服务器时，下载完数据后仍然保持连接状态。参考如下配置代码。

```
MaxKeepAliveRequests 100 #一个连接服务的最多请求次数
KeepAliveTimeout 30 #持续连接多长时间，若该连接没有再请求数据，则断开该连接。默认为
                    15 秒
```

5.1.1.2 别名设置

对于不在 DocumentRoot 指定目录内的页面，既可以使用符号连接，也可以使用别名连接。别名的设置如下。

```
Alias /download/ "/var/www/download/" #访问时可以输入 http://www.custing.com/
download/
<Directory "/var/www/download"> #对该目录进行访问控制设置
Options Indexes MultiViews
AllowOverride AuthConfig
Order allow,deny
Allow from all
</Directory>
```

5.1.1.3 CGI 设置

通过 http://www.clusting.com/cgi-bin/可以访问 ScriptAlias /cgi-bin/ "/mnt/software/ apache2/cgi-bin/"。但是，该目录下的 CGI 脚本文件要加可执行权限，设置如下。

```
<Directory "/usr/local/apache2/cgi-bin"> #设置目录属性
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>
```

5.1.1.4 日志的设置

1. 错误日志的设置

```
ErrorLog logs/error_log #日志的保存位置
LogLevel warn #日志的级别
```

显示的格式如下。

```
[Mon Oct 10 15:54:29 2005] [error] [client 192.168.10.22] access to /download/
failed, reason: user admin not allowed access
```

2. 访问日志设置

日志的默认格式有如下几种。

```
LogFormat "%h %l %u %t "%r" %>s %b "%{Referer}i" "%{User-Agent}i" " combined
LogFormat "%h %l %u %t "%r" %>s %b" common #common 为日志格式名称
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
CustomLog logs/access_log common
```

格式中各个参数的意义如下。

- %h：客户端的 IP 地址或主机名。
- %l：由客户端 identd 判断的 RFC1413 身份，输出中的符号“-”表示此处信息无效。

- %u：由 HTTP 认证系统得到的访问该网页的客户名。有认证时才有效，输出中的符号“-”表示此处信息无效。
- %t：服务器完成对请求的处理所用的时间。
- “%r”：引号中是客户发出的包含了许多有用信息的请求内容。
- %>s：服务器返回给客户端的状态码。
- %b：返回给客户端的不包括响应头的字节数。
- "%{Referer}i"：此项指明了该请求是从哪个网页提交过来的。
- "%{User-Agent}i"：此项是客户浏览器提供的浏览器识别信息。

5.1.1.5　用户认证的配置

1. httpd.conf 文件的配置

假定对目录/var/www/download 下的文件需要做 Apache 用户认证，则在 httpd.conf 中加入下面的代码：

```
AccessFileName .htaccess
…
Alias /download/ "/var/www/download/"
<Directory "/var/www/download">
Options Indexes
AllowOverride AuthConfig
</Directory>
```

2. create a password file

Apache 自带的 htpasswd 提供了建立和更新存储用户名、密码口令文件的功能，其配置语句如下：

```
/usr/local/apache2/bin/htpasswd -c /var/httpuser/passwords bearzhang
Configure the server to request a password and tell the server which users
are allowed access.
vi /var/www/download/.htaccess:
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /var/httpuser/passwords
Require user bearzhang
#Require valid-user #all valid user
```

5.1.1.6　用户认证的虚拟主机的配置

1. 基于 IP 地址的虚拟主机配置

基于 IP 地址的虚拟主机配置代码如下：

```
Listen 80
<VirtualHost 172.20.30.40>
DocumentRoot /www/example1
ServerName www.example1.com
</VirtualHost>
```

```
<VirtualHost 172.20.30.50>
DocumentRoot /www/example2
ServerName www.example2.org
</VirtualHost>
```

2. 基于 IP 和多端口的虚拟主机配置

基于 IP 和多端口的虚拟主机配置代码如下：

```
Listen 172.20.30.40:80
Listen 172.20.30.40:8080
Listen 172.20.30.50:80
Listen 172.20.30.50:8080

<VirtualHost 172.20.30.40:80>
DocumentRoot /www/example1-80
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.40:8080>
DocumentRoot /www/example1-8080
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.50:80>
DocumentRoot /www/example2-80
ServerName www.example1.org
</VirtualHost>

<VirtualHost 172.20.30.50:8080>
DocumentRoot /www/example2-8080
ServerName www.example2.org
</VirtualHost>
```

3. 单个 IP 地址的服务器上基于域名的虚拟主机配置

单个 IP 地址的服务器上基于域名的虚拟主机配置代码如下：

```
# Ensure that Apache listens on port 80
Listen 80

# Listen for virtual host requests on all IP addresses
NameVirtualHost *:80

<VirtualHost *:80>
DocumentRoot /www/example1
ServerName www.example1.com
ServerAlias example1.com. *.example1.com
# Other directives here
</VirtualHost>
```

```
<VirtualHost *:80>
DocumentRoot /www/example2
ServerName www.example2.org
# Other directives here
</VirtualHost>
```

4. 在多个 IP 地址的服务器上配置基于域名的虚拟主机

在多个 IP 地址的服务器上配置基于域名的虚拟主机的代码如下：

```
Listen 80

# This is the "main" server running on 172.20.30.40
ServerName server.domain.com
DocumentRoot /www/mainserver

# This is the other address
NameVirtualHost 172.20.30.50

<VirtualHost 172.20.30.50>
DocumentRoot /www/example1
ServerName www.example1.com
# Other directives here ...
</VirtualHost>

<VirtualHost 172.20.30.50>
DocumentRoot /www/example2
ServerName www.example2.org
# Other directives here ...
</VirtualHost>
```

5. 在不同的端口上运行不同的站点(基于多端口的服务器上配置基于域名的虚拟主机)

实现在不同的端口上运行不同站点的配置代码如下：

```
Listen 80
Listen 8080

NameVirtualHost 172.20.30.40:80
NameVirtualHost 172.20.30.40:8080

<VirtualHost 172.20.30.40:80>
ServerName www.example1.com
DocumentRoot /www/domain-80
</VirtualHost>

<VirtualHost 172.20.30.40:8080>
ServerName www.example1.com
DocumentRoot /www/domain-8080
</VirtualHost>
```

```
<VirtualHost 172.20.30.40:80>
ServerName www.example2.org
DocumentRoot /www/otherdomain-80
</VirtualHost>

<VirtualHost 172.20.30.40:8080>
ServerName www.example2.org
DocumentRoot /www/otherdomain-8080
</VirtualHost>
```

6. 基于域名和基于 IP 的混合虚拟主机的配置

基于域名和基于 IP 的混合虚拟主机的配置代码如下：

```
Listen 80
NameVirtualHost 172.20.30.40

<VirtualHost 172.20.30.40>
DocumentRoot /www/example1
ServerName www.example1.com
</VirtualHost>

<VirtualHost 172.20.30.40>
DocumentRoot /www/example2
ServerName www.example2.org
</VirtualHost>

<VirtualHost 172.20.30.40>
DocumentRoot /www/example3
ServerName www.example3.net
</VirtualHost>
```

5.1.2 典型例题分析

例 1 阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】某公司搭建了一个小型局域网，局域网内有 200 台 PC，网络中配置一台 Linux 服务器作为 Internet 接入服务器，Linux 服务器 E0 网卡的 IP 地址为 192.168.1.1，E1 网卡的 IP 地址为 202.100.20.30，该网络结构如图 5-1 所示。

为了方便局域网 IP 管理，决定在 Linux Server 中配置 DHCP 服务，要求 DHCP 服务的配置满足以下几个条件：

1. 考虑今后扩展需求，当前只使用 192.168.1.1～192.168.1.201 的 IP 地址。

2. PC100(MAC 地址为 00:A0:78:8E:9E:AA)作为内部文件服务器，需要使用固定的 IP 地址为 192.168.1.100。

3. 在 Linux Server 上配置 DNS 服务。

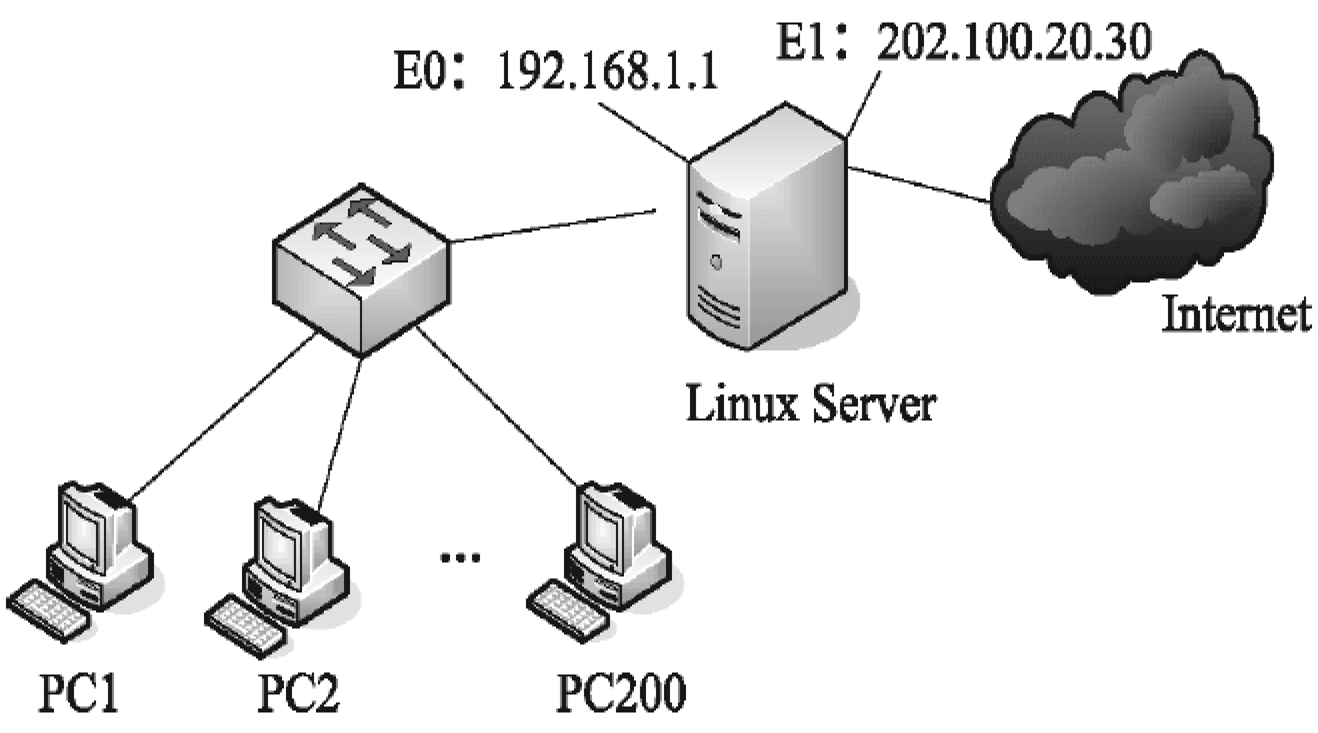


图 5-1　网络结构

【问题 1】(9 分)

根据题目要求补充完成 DHCP 服务器配置文件 dhcpd.conf 的配置项。

```
default-lease-time 1200;
max-lease-time 9200;
option subnet-mask 255.255.255.0
option broadcast-address _(1)_;
option routers _(2)_;
option domain-name-services _(3)_;
subnet _(4)_ netmask _(5)_
{
        range _(6)_ _(7)_;
{
   host fixed {
   hardware ethernet _(8)_;
 fixed address _(9)_;
}
```

【问题 2】(4 分)

根据 DHCP 协议约定和问题 1 的配置，DHCP 客户端 PC1 从获取 IP 地址后经过 (10) 分钟需要到 DHCP 服务器申请租约更新。此时 PC1 发送到 DHCP 服务器的消息是 (11) 。如果 DHCP 服务器同意租约更新，响应的消息是 (12) 。如果 DHCP 服务器不同意租约更新，响应的消息是 (13) 。

【问题 3】(2 分)

在 DHCP 客户端，还可以通过 Windows 命令 (14) 来立即释放申请到的 IP 地址，通过命令 (15) 来立即重新申请租约。

答案：

【问题 1】

(1) 192.168.1.255　(2) 192.168.1.1　(3) 192.168.1.1　(4) 192.168.1.0

(5) 255.255.255.0　(6)192.168.1.2　(7) 192.168.1.201

(8) 00:A0:78:8E:9E:AA　(9) 192.168.1.100

【问题 2】

(10) 10　(11) DHCPQUEST　(12) DHCPACK　(13) DHCPNACK

【问题 3】

(14) ipconfig /release　(15) ipconfig /renew

解析：

【问题 1】 在 Linux 系统中，DHCP 服务的服务器程序是 dhcpd，该程序以独立方式启动运行，其配置文件是/etc/dhcpd.conf，在这个文件中定义了默认租期、最大租期、可分配的 IP 地址范围、子网掩码以及网关、名字服务器等选项。由题知，指定广播地址为 192.168.1.255，指明子网内的默认网关(即路由器)的地址为 192.168.1.1，在 Linux Server 上配置 DNS 服务，故指明 DNS 服务器的地址为 192.168.1.1。因为局域网内有 200 台主机，所以子网为 192.168.1.0，子网掩码为 255.255.255.0。考虑今后扩展需求，当前只使用 192.168.1.1～192.168.1.201 的 IP 地址；因此指明要分配的 IP 地址的范围从 192.168.1.2～192.168.1.201。

PC100(MAC 地址为 00:A0:78:8E:9E:AA)作为内部文件服务器，需要使用固定的 IP 地址为 192.168.1.100，故 MAC 地址为 00:A0:78:8E:9E:AA 的主机配置固定的 IP 地址 192.168.1.100。

【问题 2】 DHCP 服务器向 DHCP 客户机出租的 IP 地址一般都有一个租借期限，期满后 DHCP 服务器便会收回出租的 IP 地址。如果 DHCP 客户机要延长其 IP 租约，则必须更新其 IP 租约。DHCP 客户机启动时和 IP 租约期限过一半时，DHCP 客户机都会自动向 DHCP 服务器发送更新其 IP 租约的信息。依据问题 1 的配置，可知指定默认租约时间 1200s，就是 20 分钟，DHCP 客户端 PC1 从获取 IP 地址后经过 10 分钟需要到 DHCP 服务器申请租约更新。此时 PC1 发送到 DHCP 服务器的消息是 DHCPQUEST。如果 DHCP 服务器同意租约更新，响应的消息是 DHCPACK。如果 DHCP 服务器不同意租约更新，响应的消息是 DHCPNACK。

【问题 3】Windows XP 用户可以通过 ipconfig /all 命令看出自己申请到的本机 IP 地址；使用 ipconfig /renew 命令重新向 DHCP 服务器申请 IP 地址；使用 ipconfig /release 命令释放 IP 地址。

例 2　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】 某公司搭建了一个小型局域网，网络中配置一台 Linux 服务器作为公司内部文件服务器和 Internet 接入服务器，该网络拓扑结构如图 5-2 所示。

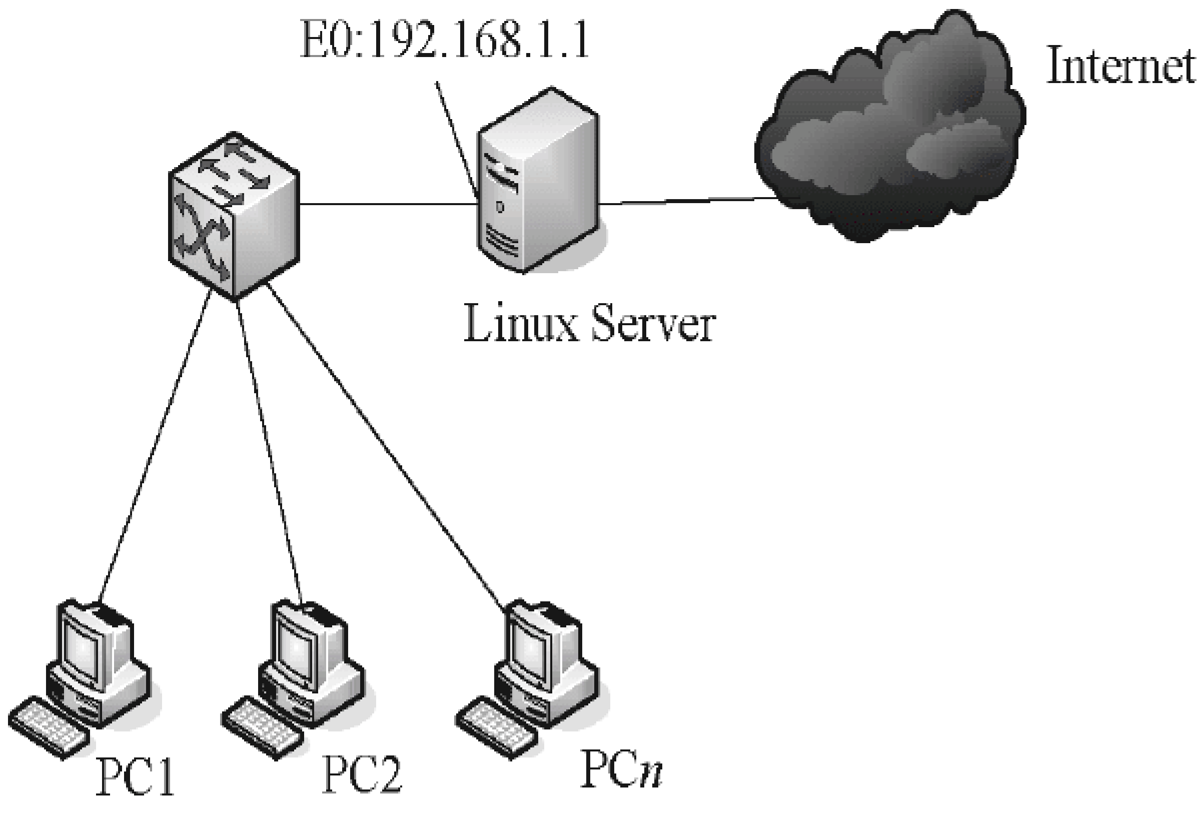


图 5-2　网络拓扑结构

【问题 1】(5 分)

Linux 的文件传输服务是通过 vsftpd 提供的，该服务使用的应用层协议是 (1) 协议，传

输层协议是 (2) 协议，默认的传输层端口号为 (3) ，vsftpd 服务可以通过命令行启动或停止，启动该服务的命令是 (4) ，停止该服务的命令是 (5) 。

【问题 2】(5 分)

vsftpd 程序主配置文件的文件名是 (6) 。若当前配置内容如下所示，请给出对应配置项和配置值的含义。

```
…
listen_address=192.168.1.1
#listen_port=21
#max_per_ip=10
#max_clients=1000
anonymous_enable=YES      (7)
local_enable=YES          (8)
write_enable=YES          (9)
userlist_enable=YES       (10)
…
```

【问题 3】(2 分)

为了使因特网上的用户也可以访问 vsftpd 提供的文件传输服务，可以通过简单地修改上述主配置文件来实现，修改的方法是 (11) 。

【问题 4】(3 分)

由于 Linux 服务器的配置较低，希望限制同时使用 FTP 服务的并发用户数为 10，每个用户使用 FTP 服务时建立的连接数为 5，可以通过简单地修改上述主配置文件来实现，修改的方法是 (12) 。

答案：

【问题 1】

(1) FTP　(2) TCP　(3) 21　(4) service vsftpd start　(5) service vsftpd stop

【问题 2】

(6) vsftpd.conf　(7) 允许匿名用户访问　(8) 允许本地用户访问

(9) 允许用户上传文件　(10) 禁止用户列表文件中的用户访问

【问题 3】

(11) 注释或删除“listen_address=192.168.1.1”配置项

【问题 4】

(12) 改“#max_per_ip=10”为“#max_per_ip=5”，改“#max_clients=1000”为“#max_clients=10”

解析：

【问题 1】 FTP 主要用来在计算机之间传输文件，工作在应用层；TCP 协议在 IP 协议软件提供的服务的基础上，支持面向连接的、可靠的、面向流的投递服务，工作在传输层，默认传输层端口号是 21；启动服务输入命令为 service vsftpd start；停止服务输入命令为 service vsftpd stop。

【问题 2】配置文件的后缀名为.conf，故 vsftpd 程序主配置文件的文件名为 vsftpd.conf。anonymous_enable=YES 表示允许匿名用户访问；local_enable=YES 表示允许本地用户访问；

write_enable=YES 表示允许用户上传文件；userlist_enable=YES 表示禁止用户列表文件中的用户访问。

【问题 3】 要使因特网上的用户也可访问 vsftpd 提供的文件传输服务，则可将固定的访问地址删除，即注释或删除“listen_address=192.168.1.1”配置项。

【问题 4】 max-per-ip 表示每个客户机的最大连接数，题目要求每个用户使用 FTP 服务时可建立的连接数为 5，则将“#max_per_ip=10”改为“#max_per_ip=5”，限制同时使用 FTP 服务的并发用户数为 10，将“#max_clients=1000”改为“#max_clients=10”。

例 3 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2011 年下半年下午试题二)

【说明】 如图 5-3 所示，某公司办公网络划分为研发部和销售部两个子网，利用一台双网卡 Linux 服务器作为网关，同时在该 Linux 服务器上配置 Apache 提供 Web 服务。

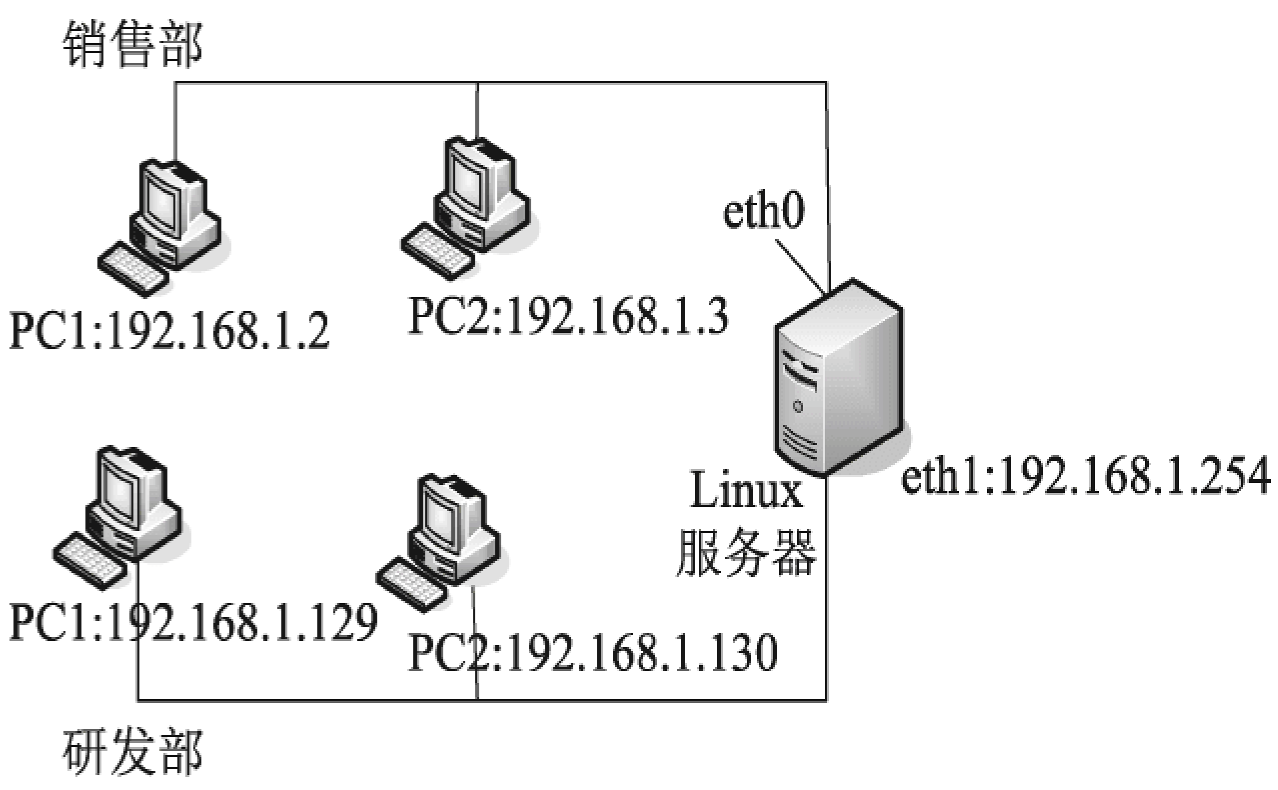


图 5-3　网络规划图

【问题 1】

图 5-4 是 Linux 服务器中网卡 eth0 的配置信息，从图中可以得知：①处输入的命令是__(1)__，eth0 的 IP 地址是__(2)__，子网掩码是__(3)__，销售部子网最多可以容纳的主机数是__(4)__。

```
    [root@localhost conf]#__①__
    eth0      Link encap:Ethernet Hwaddr 00:29:C8:0D:10
              inet addr:192.168.1.126 Bcast:192.168.1.255
Mask:255.255.255.128
              UP HROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:1667 errors:0 dropped:0 overruns:0 frame:0
              TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:100
              RX bytes:291745(284.9KB) TX bytes:924(924.0b)
              Interrupt:10 Base address:0x10a4
```

图 5-4　eth0 的配置信息

【问题 2】

Linux 服务器配置 Web 服务之前，执行命令[root@root]rpm-qa|grep httpd 的目的是__(5)__。Web 服务器配置完成后，可以用命令__(6)__来启动 Web 服务。

【问题 3】

默认安装时，Apache 的主配置文件名是 (7) ，该文件所在目录为 (8) 。

配置文件中下列配置信息的含义是 (9) 。

```
<Directory "/var/www/html/secure">
AllowOverride AuthConfig
Order deny allow
Allow from 192.168.1.2
Deny from all
</Directory>
```

【问题 4】

Apache 的主配置文件中有一行 Listen 192.168.1.126:80，其含义是 (10) 。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务。在 Linux 服务器中应如何配置，方能使研发部的主机也可以访问 Web 服务？

答案：

【问题 1】

(1) ifconfig eth0 或 ifconfig

(2) 192.168.1.126

(3) 255.255.255.128

(4) 125

【问题 2】

(5) 确认 Apache 软件包是否已经成功安装

(6) service httpd start

【问题 3】

(7) httpd.conf

(8) /etc/httpd/conf

(9) 目录“/var/www/html/secure”只允许主机 192.168.1.2 访问

【问题 4】

(10) 提供 Web 服务的地址是 192.168.1.126，端口是 80

将 Apache 主配置文件中的配置“Listen 192.168.1.126:80”修改为“Listen 80”，或者增加从研发部网络到销售部网络的路由。

解析：

【问题 1】 配置主机网络接口命令为 ifconfig。

程序/sbin/ifconfig 用来配置主机网络接口。这包括基本的配置，如 IP 地址、掩码和广播地址，以及高级的选项，如为点对点连接(如 PPP 连接)设置远程地址。

一个接口可以在不进行重新配置的情况下临时地变为不可用和再变为可用。接口可以用于将服务器的网络连接临时变为不可用(当重新配置一个服务时)。使用下列命令可实现本功能。

```
ifconfig interface down    关闭接口
ifconfig interface ip-address up 启动接口
```

图 5-4 中显示以太网接口地址为 192.168.1.126，子网掩码为 255.255.255.128。

由于销售部的以太网接口地址为 192.168.1.126，而 192.168.1.1 不能用，所以其可用地址范围为 192.168.1.2～192.168.1.126，可连接主机数为 125 台。

【问题 2】 “|” 是 Linux 很有用的一个用法，俗称管道，可把一个命令的输出作为下个命令的输入。

rmp –qa 中的 “-q” 表示查找；“-a” 表示 all(所有)；grep 为正则表达匹配；所以，这个命令的含义就是 “查找所有和 HTTPD 服务相关的”，即列出所有装配的软件。

Apache 的启动命令为 service httpd start。

【问题 3】 Apache 的主配置文件名是 httpd.conf，该文件所在目录为/etc/httpd/conf。

<Directory "/var/www/html/secure">指进入此目录；AllowOverride AuthConfig 即允许该目录对 AuthConfig 属性进行覆盖；后面几句即允许指定 IP 访问，而不允许其他 IP 访问。所以语句的整体意思为目录 “/var/www/html/secure” 只允许主机 192.168.1.2 访问。

【问题 4】 Listen 语句的意思是允许将 Apache 绑定到指定的 IP 地址和端口，作为默认值的辅助选项。则其含义为提供 Web 服务的地址是 192.168.1.126，端口是 80。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务，要使研发部的主机也可以访问 Web 服务，则需要增加从研发部网络到销售部网络的路由，或者将主配置文件中的配置 “Listen 192.168.1.126:80” 修改为 “Listen 80”。

例 4 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2011 年上半年下午试题二)

【说明】 Linux 系统有其独特的文件系统 ext2，文件系统包括文件的组织结构、处理文件的数据结构及操作文件的方法。可以通过命令获取系统及磁盘分区状态信息，并能对其进行管理。

【问题 1】(6 分)

以下命令中，改变文件所属群组的命令是__(1)__，编辑文件的命令是__(2)__，查找文件的命令是__(3)__。

(1)～(3)备选答案：

A. chmod　　B. chgrp　　C. vi　　D. which

【问题 2】(2 分)

在 Linux 中，伪文件系统__(4)__只存在于内存中，通过它可以改变内核的某些参数。

A. /proc　　B. ntfs　　C. /tmp　　D. /etc/profile

【问题 3】(4 分)

在 Linux 中，分区分为主分区、扩展分区和逻辑分区，使用 fdisk -l 命令获得的分区信息如下所示。

```
Disk /dev/hda:240 heads, 63 sectors, 140 cylinders
Units=cylinders of 15120 * 512 bites
Device Boot       Start      End      Blocks      Id      System
/dev/hda          1          286      2162128+    c       Win95 FAT32(LBA)
/dev/hda2    *    288        1960     12496680    5       Extended
/dev/hda5         288        289      15088+      83      Linux
```

```
/dev/hda6       290       844       4195768+    83      Linux
/dev/hda7       845       983       1050808+    82      Linux swap
/dev/hda8       984       1816      6297448+    83      Linux
/dev/hda9       1817      1940      937408+     83      Linux
```

其中，属于扩展分区的是＿(5)＿。

使用 df -T 命令获得的信息部分如下所示。

```
Filesystem  Type      1k Blocks   Used      Avallable    Use%   Mounted on
/dev/hda6   relserfs  4195632     2015020   2180612      49%    /
/dev/hda5   ext2      14607       3778      10075        8%     /boot
/dev/hda9   relserfs  937372      202368    735004       22%    /home
/dev/hda8   relserfs  6297248     3882504   2414744      62%    /opt
Shmfs       shm       256220      0         256220       0%     /dev/shm
/dev/hda1   vfat      2159992     1854192   305800       86%    /windows/c
```

其中，不属于 Linux 系统分区的是＿(6)＿。

【问题 4】(3 分)

在 Linux 系统中，对于＿(7)＿文件中列出的 Linux 分区，系统启动时会自动挂载。此外，超级用户可以通过＿(8)＿命令将分区加载到指定目录，从而该分区才在 Linux 系统中可用。

答案：

【问题 1】

(1) B　(2) C　(3) D

【问题 2】

(4) A

【问题 3】

(5) /dev/hda2　(6) Shmfs

【问题 4】

(7) /etc/fstab　(8) mount

解析：

【问题 1】改变文件所属群组的命令是 chown 或者 chgrp，其中 chgrp 是专门改群组的。编辑文件的命令是 vi。(3)中 which 应该是查找命令的可执行文件所在的位置。

【问题 2】 proc 文件系统是一个伪文件系统，它只存在于内存中，而不占用外存空间。它以文件系统的方式为访问系统内核数据的操作提供接口。用户和应用程序可以通过 proc 得到系统的信息，并可以改变内核的某些参数。由于系统的信息，如进程，是动态改变的，所以用户或应用程序读取 proc 文件时，proc 文件系统是动态地从系统内核读出所需信息并提交的。

【问题 3】

(5) 的答案可以在图中找出，hda2 后面写的是 Extended。

(6) 中的 Shmfs 文件系统是一种内存共享模式的文件系统。

【问题 4】 本题考查 Linux 文件系统常识和基本操作命令。

在 Linux 系统中，对于/etc/fstab 文件中列出的 Linux 分区，系统启动时会自动挂载。此

外，超级用户可以通过 mount 命令将分区加载到指定目录，从而该分区才在 Linux 系统中可用。

5.1.3　同步练习

阅读以下关于在 Linux 系统中配置 Apache 服务器的说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】 在 Linux 系统中采用 Apache 配置 Web 服务器。Apache 服务器提供了丰富的功能，包括目录索引、目录别名、虚拟主机、HTTP 日志报告、CGI 程序的 SetUID 执行等。

【问题 1】(6 分)

请在(1)～(4)空白处填写恰当的内容。

Web 客户机与服务器共同遵守 (1) 协议，其工作过程是：Web 客户端程序根据输入的 (2) 连接到相应的 Web 服务器上，并获得指定的 Web 文档。动态网页以 (3) 程序的形式在服务器端处理，并给客户端返回 (4) 格式的文件。

(1)～(4)备选答案：

A. HTML	B. ASP	C. JSP	D. IIS
E. SOAP	F. URL	G. HTTP	H. VGA

【问题 2】(7 分)

请在(5)～(11)空白处填写恰当的内容。

Apache 的主配置文件为 httpd.conf。某 Web 服务器的 httpd.conf 文件部分内容如下。

```
ServerType standalone
ServerRoot "/etc/httpd"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MinSpareServer 5
MaxSpareServer 20
StartServer 8
MaxClients 150
MaxRequestsPerChild 100
Port 8080
User nobody
Group nobody
ServerAdmin root@webtest.com.cn
ServerName WebText
DocumentRoot "/home/webtest/jakarta-tomcat/webapps/webtest"
Options FollowSymLinks
AllowOverride None
Options Indexes Includes FollowSymLinks
AllowOverride None
Order allow,deny
```

```
Allow from all
DirectoryIndex index.html index.htm index.shtml index.cgi
Alias/doc//usr/doc
order deny,allow
deny from all
allow from localhost
Options Indexes FollowSymLinks
```

以 RPM 方式安装的 Apache 服务器，配置文件 httpd.conf 存储在 Linux 的 (5) 目录下。根据上述配置文件，该 Web 服务器运行在 (6) 模式下，其运行效率比在 inetd 模式下 (7) ；当某个 Web 连接超过 (8) 秒没有数据传输时，系统断开连接。

如果客户需要访问 Linux 服务器上的/usr/doc 目录，则应在浏览器地址栏中输入 (9) 。

虚拟主机是指在同一服务器上实现多个 Web 站点。虚拟主机可以是基于 IP 地址的虚拟主机，也可以是基于 (10) 的虚拟主机。创建基于 (10) 的虚拟主机时，还需要配置 (11) ，并在数据库文件中添加相关记录。

【问题 3】(2 分)

图 5-5 是配置 Apache 服务器的一个对话框，选中目录选项 ExecCGI，意味着什么？

如果将图 5-5 所示的目录选项中 Indexes 的选中状态取消，并且虚拟主机目录中也没有相关的 Index 文件，客户机通过浏览器访问有关的虚拟主机目录时有何结果？

图 5-5　“目录选项”对话框

5.1.4　同步练习参考答案

答案：

【问题 1】

(1)　G　　(2)　F　　(3)　C　　(4)　A

【问题 2】

(5)　/etc/httpd/conf　　(6)　standalone　　(7)　高　　(8)　300

(9)　http://服务器 IP 地址(或主机名):8080/doc/

(10) 名称(或名字，域名)

(11) DNS 或域名解析服务

【问题 3】

选中目录选项 ExeceCGI，意味着准许执行 CGI。

如果将 Indexes 选中状态取消，则不允许客户机浏览器在虚拟主机没有 Index 文件时显示目录所有文件。

5.2 DNS 服务器的配置

5.2.1 考点辅导

5.2.1.1 DNS 服务器的类型

在 Linux 中，域名服务(DNS)是由柏克莱网间域名(Berkeley Internet Name Domain，BIND)软件实现的。BIND 是一个客户/服务系统，它的客户方面称为转换程序(Resolver)，它产生域名信息的查询，将这类信息发送给服务器，DNS 软件回答转换程序的查询。BIND 的服务方面是一个称为 named 的守护进程。

BIND 可以配置成以几种不同的方法运行的 DNS，常见的 BIND 配置是唯转换程序系统、唯高速缓存服务器、主服务器和辅助域名服务器。

- 唯转换程序系统：转换程序是一段要求域名服务器提供域信息的程序，在 Linux 系统中，它是作为一个库程序来实现的，而不是一个单独的客户程序。在唯转换程序系统中，仅使用转换程序，并不运行域名服务器。这种系统是很容易配置的，最多只需要设置/etc/resolv.conf 文件，其他三个 BIND 配置选项都是用于 named 服务软件的。
- 唯高速缓存服务器：唯高速缓存服务器(Caching-only Server)可运行域名服务器软件，但是它本身没有域名数据库软件。它从某个远程服务器上取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。所有的域名服务器都按这种方式使用高速缓存中的信息，但唯高速缓存服务器则依赖于这一技术提供所有的域名服务器信息。唯高速缓存服务器不是权威性服务器，因为它提供的所有信息都是间接信息。对于唯高速缓存服务器通常只需要配置一个高速缓存文件，但最常见的配置还包括一个回送文件，这或许才是最常见的域名服务器配置；接着是唯转换程序配置，它是最容易配置的，在 5.2.1.3 节将会详细介绍。
- 主服务器：主服务器(Primary Name Server)是特定域所有信息的权威性信息源。它从域管理员构造的本地磁盘文件中加载域信息，该文件(区文件)包含主服务器中具有管理权的一部分域最精确的结构信息。主服务器是一种权威性服务器，因为它以绝对的权威去回答对它域的任何查询。配置主服务器需要一整套配置文件，包括正规域的区文件(named.hosts)、反向域的区文件(named.rev)、引导文件(named.conf)、高速缓存(named.ca)和回送文件(named.local)，其他的配置都不需要这样一整套文件。
- 辅助域名服务器：辅助域名服务器(Secondary Name Server)可从主服务器中转移一整套域信息。区文件是从主服务器中转移出来的，并作为本地磁盘文件存储在辅助服务器中。这种转移称为“区文件转移”。在辅助域名服务器中有一个所有域信息的完整备份，可以有权威地回答对该域的查询，因此，辅助域名服务器也称

作权威性服务器。配置辅助域名服务器不需要生成本地区文件，因为可以从主服务器下载该区文件。然而其他的文件却是需要的，包括引导文件、高速缓存文件和回送文件。

一个域名服务器可以是这类配置中的任何一种，但经常是将多种配置类型的元素组合在一起，所有的系统都要运行转换程序。

5.2.1.2　配置转换程序

使用 DNS 的第一步是在用户的计算机上配置转换程序，即让机器能够从 DNS 服务器中获取域名解析/反解析服务。转换程序不是一个单独而明确的处理进程，而是网络进程调用的一个标准 C 程序库。如果本地系统不运行 named，就必须配置本地转换程序。

1. 转换程序控制文件/etc/host.conf

/etc/host.conf 是用来控制本地转换程序文件的设置文件。该文件告诉转换程序使用哪些服务、按照什么顺序进行。该文件的字段可以用空格或制表符分隔。字符“#”表示注释行。/etc/host.conf 文件的配置选项如下。

- order：指定按照哪种顺序来尝试不同的名字解析机制，按列出的顺序来进行指定的解析服务，支持下面的名字解析机制。
  - hosts：试图通过查找本地/etc/hosts 文件来解析主机名字。
  - bind：使用 DNS 域名服务器来解析主机名字。
  - nis：使用网络信息服务(NIS)协议来解析主机名字。
- multi：以 off 和 on 为参数。与 host 查询一起使用，用来确定一台主机是否在/etc/hosts 文件中指定了多个 IP 地址。
- nospoof：如果用逆向解析找出与指定的地址匹配的主机名，就可以对返回的地址进行解析以确认它确实与查询的地址相配。为了防止“骗取”IP 地址，可通过指定 nospoof on 来允许逆向解析功能。
- alert：以 off 和 on 为参数。如果打开，任何试图骗取 IP 地址的行为都通过 syslog 工具被记录下来。
- trim：以域名为参数。在/etc/hosts 中查找名字前，trim 删除这个域名，只把基本主机名放在/etc/host.conf 中而不指定域名。

下面这个例子是主机 vlager 上的/etc/host.conf 文件。

```
# /etc/host.conf
# We have named running, but no NIS (yet)
order bind hosts
# Allow multiple addrs
multi on
# Guard against spoof attempts
nospoof on
# Trim local domain (not really necessary).
trim vbrew.com.
```

这个例子给出了域 vbrew.com 的通用解析程序配置。该解析程序首先使用 DNS 解析，然后使用/etc/hosts 文件查找主机名。在解析查找中指定本地/etc/hosts 文件是一个好主意。

如果由于某种原因不能使用域名服务器，那么还可以使用主机文件中列出的那些主机名。该机器上允许使用多个 IP 地址，主机通过重新解析主机名字(从 IP 地址逆向查找返回的主机名字)来检查 IP 欺骗。

2. 转换程序配置文件/etc/resolv.conf

当配置转换程序使用 BIND 域名服务查询主机时，必须告诉转换程序使用哪一个域名服务器。用来完成这项任务的工具就是/etc/resolv.conf 文件。/etc/resolv.conf 控制转换程序采用 DNS 解析主机名时使用的方式，可以明确地定义系统的配置，允许命名由于默认服务器不响应而使用的备份服务器。因此，尽管会增加系统负荷，但在某些场合使用 resolv.conf 还是很受欢迎的。

/etc/resolv.conf 是一个简单而易读的文件。在/etc/resolv.conf 中使用的命令，具有系统专用的形式，但一般都支持 nameserver 和 domain 两项命令。

nameserver 项利用 IP 地址去识别，让转换程序识别查询域信息的那些服务器。可以通过多次使用 nameserver 选项，使用多达三个域名服务器。这些域名服务器是按照它们在文件中的顺序进行查询的，如果没有接收到任何一个服务器的响应，则尝试表中的下一个服务器，直到所有服务器试完为止(如果在/etc/resolv.conf 文件中设置了三个以上的域名服务器，那么即使前三个服务器都没有响应查询请求，Linux 也不会去请求后面的服务器)。应该将最可靠的域名服务器列在最前面，以便在查询时不会超时。如果 resolv.conf 文件中不包含 nameserver 项，或者不存在 resolv.conf 文件，就将所有域名服务器查询发送给本地主机。然而，如果有一个 resolv.conf 文件，它包含 nameserver 项，除非有一项指向本地主机，否则就不查询本地主机。在配置唯转换程序的主机中，resolv.conf 文件包含 nameserver 项，但没有一个项指向本地主机。

domain 项用来定义默认域名(主机的本地域名)。转换程序会将默认域名挂在任何不含点的主机名后面。例如，转换程序接收到主机名 vale(它不含点)，就将其默认域名挂接在 vale 的后面，对它进行查询。如果 domain 域中的 name 值是 vbrew.com，那么转换程序就将查询 vale.vbrew.com。如果没有找出它，则转换程序就试图通过 getdomainname()系统调用来获得本地域名。

如果听起来让人迷惑不解，可以看看下面这个例子，这是 Virtual Brewery 中的 resolv.conf 文件。

```
# /etc/resolv.conf
# Our domain
domain vbrew.com
#
# We use vlager as central nameserver:
nameserver 191.72.1.1
```

在该例中，通过 domain 项指定默认域名，并列出一个用于解析主机名的域名服务器。在这个例子中没有指定查询顺序(使用 search 选项)，因此如果要查询一台机器的地址(如 vale)，解析器会首先试图查找 vale，如果没有找到，则查找 vale.vbrew.com，然后再查找 vbrew.com。

5.2.1.3 唯转换程序配置

配置唯转换程序是非常简单的，下面是一个唯转换程序的/etc/resolv.conf 文件的例子。

```
# /etc/resolv.conf
# Our domain
domain vbrew.com
#
# We use vlager as central nameserver:
nameserver 191.72.1.1
# next try vale
namesever 191.72.1.3
```

该配置文件告诉转换程序将所有的查询发送给主域名服务器 vlager，如果失败，就试 vale。这些查询是永远不能在本地转换的。这一个简单的 resolv.conf 文件就可以满足唯转换程序配置的全部要求。

5.2.1.4 设置域名服务器

在 Linux 上的域名服务是由 named 守护进程来执行的，named 最早是为 BSD 向客户机提供域名服务而开发的。named 守护进程通常在系统启动时开始工作，并一直工作到系统关闭。该进程从被称作/etc/named.boot 的配置文件中获取有关信息，并将主机名映射为 IP 地址的各种文件。

只要在命令行中输入# /etc/rc.d/init.d/named start, named 就会开始运行，读取 named.boot 文件及其定义的任意区文件，并将它的进程 ID 以 ASCII 码的形式写入/var/run/named.pid 中，下载任何来自主服务器的区文件，如果有必要的话在端口 53 等待 DNS 请求。

下面介绍与 DNS 有关的几个配置文件以及它们的功能。

- named.conf：设置一般的 named 参数，指向该服务器使用的域数据库信息的源，这类源可以是本地磁盘文件或远程服务器。
- named.ca：指向根域名服务器。
- named.local：用于在本地转换回送地址。
- named.hosts：将主机名映射为 IP 地址。
- named.rev：用于反向域的、将 IP 地址映射到主机名的区文件。

理解不同配置的最佳方法是讨论各种 named.conf 的示例文件。

1. 唯高速缓存服务器的配置

配置唯高速缓存域名服务器是很简单的，必须有 named.conf 和 named.ca 文件，通常也要用到 named.local 文件。下面是用于唯高速缓存服务器的 named.conf 文件的例子，其中以“//”开头的是注释。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
```

```
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
//
// a caching only nameserver config
//
zone "." {
type hint;
file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
```

directory 这一行告诉 named 到哪里去找寻文件，所有其后命名的文件都是相对于此目录的。该文件告诉 named 维持一个域名服务器响应的高速缓存，并利用 named.ca 文件的内容初始化该高速缓存。该高速缓存初始化文件的名字可以是任何名字，但一般使用/var/named/named.ca。并不是在该文件中使用一个 hint 语句就能使它成为唯高速缓存配置，而是因为没有 master 和 slave 语句才使它成为一个唯高速缓存配置文件。

但是，在这个例子中却有一个 master 语句。事实上，几乎在每一个唯高速缓存的配置文件中都有这一语句，它将本地服务器定义为它自己的回送域的主服务器，并假定该域的信息存储在 named.local 文件中。这个回送域是一个 in-addr.arpa 域(in-addr.arpa 域用于指定逆向解析，或 IP 地址到 DNS 名字解析)，它将地址 127.0.0.1 映射为名字 localhost。转换自己的回送地址对于大多数人都是有意义的，因为许多 named.conf 文件都包含这一项。

在大多数唯高速缓存服务器的配置文件中，这种 directory、master 和 hint 语句是唯一使用的语句，但也可以增加其他的语句，比如 forwarders 和 slave 等语句都可以使用。

2. 主服务器和辅助服务器的配置

我们虚构的 vbrew.com 用于说明主服务器和辅助服务器的基础，下面是将 vlager 定义为 vbrew.com 域主服务器的 named.conf 文件。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
```

```
};
//
// a caching only nameserver config
//
zone "." {
type hint;
file "named.ca";
};
zone "vbrew.com"{
type master;
file "named.hosts";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
zone "72.191.in-addr.arpa"{
type master;
file "named.rev";
};
```

上例中第一个 master 说明这是 vbrew.com 域的主服务器。该域的数据是从 named.hosts 文件中加载的。在这个例子中，我们可以将文件名 named.hosts 作为区文件名，也可以使用更有说明性的文字，例如，vbrew.com 区文件的名字使用 vbrew.com.hosts 则较好。

第三个 master 语句指向能将 IP 地址 191.72.0.0 映射为主机名的文件。它假定本地服务器是反向域 72.191.in-addr.arpa 的主服务器，该域的数据从文件 named.rev 中加载。

对于上例配置中的 hint 语句我们在前面唯高速缓存配置中已经讨论过。在这些配置中，它们的作用是相同的，而且几乎在任何配置中都要使用它们。

辅助服务器的配置与主服务器的配置不同，它使用 slave 语句代替 master 语句。slave 语句指向用作域信息源的远程服务器，以替代本地磁盘文件。下面的 named.conf 文件可以将 vale 配置成 vbrew.com 域的辅助服务器。

```
// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
//
// a caching only nameserver config
//
```

```
zone "." {
type hint;
file "named.ca";
};
zone "0.0.127.in-addr.arpa"{
type master;
file "named.local";
};
zone "vbrew.com"{
type slave;
file "named.hosts";
masters { 191.72.1.3; };
};
zone "72.191.in-addr.arpa"{
type slave;
file "named.rev";
masters {191.72.1.3;};
};
cache . named.ca
secondary vbrew.com 191.72.1.3 named.hosts
secondary 72.191.in-addr.arpa 191.72.1.3 named.rev
primary 0.0.127.in-addr.arpa named.local
```

第一个 slave 语句是使这个服务器成为 vbrew.com 的辅助服务器。它告诉 named 从 IP 地址为 191.72.1.3 的服务器中下载 vbrew.com 的信息，并将其数据保存在/var/named/named.hosts 文件中。如果该文件不存在，named 就创造一个，并从远程服务器中取得区数据，然后将这些数据写入新创建的文件中。如果存在该文件，named 就要检查远程服务器，以了解远程服务器的数据是否不同于该文件中的数据。如果数据有变化，它就下载更新后的数据，用新数据覆盖该文件的内容；如果数据没有变化，named 就加载磁盘文件的内容，而不必做麻烦的区转移工作。

将一个数据库复制到本地磁盘文件中，就不必在每次引导主机时都要转移区文件；只有当数据修改时，才进行这种区文件的转移工作。

配置文件中的下一行表示该本地服务器也是反向域 72.191.in-addr.arpa 的一个辅助服务器，而且该域的数据也从 191.72.1.3 中下载。反向域的数据存储在 named.rev 中。

DNS 数据库文件和资源记录配置 named 所需的所有文件(named.hosts、named.rev、named.local 和 named.ca)中的信息都是以资源记录的形式存在的。每个资源记录都有一个类型，这个类型说明记录的功能。这些记录都是标准资源记录，称为 RR(Resource Records)。

5.2.2 典型例题分析

【说明】(2014 年上半年下午试题三)

某单位网络拓扑结构如图 5-6 所示，在 Linux 系统下构建 DNS 服务器、DHCP 服务器和 Web 服务器。要求如下。

1. 路由器连接各个子网的接口信息如下：

(1)　路由器 E0 的 IP 地址 192.168.1.1/25。

(2)　路由器 E1 的 IP 地址 192.168.1.129/25。

(3)　路由器 E2 的 IP 地址 192.168.2.1/25。

(4)　路由器 E3 的 IP 地址 192.168.2.33/25。

2. 子网 1 和子网 2 内的客户机通过 DHCP 服务器动态分配 IP 地址。

3. 服务器设置固定的 IP 地址，其中：

(1)　DNS 服务器采用 BIND 构建，IP 地址为 192.168.2.2。

(2)　DHCP 服务器的 IP 地址为 192.168.2.3。

(3)　Web 服务器网卡 eth0 的 IP 地址为 92.168.2.4，eth1 的 IP 地址为 92.168.2.34。

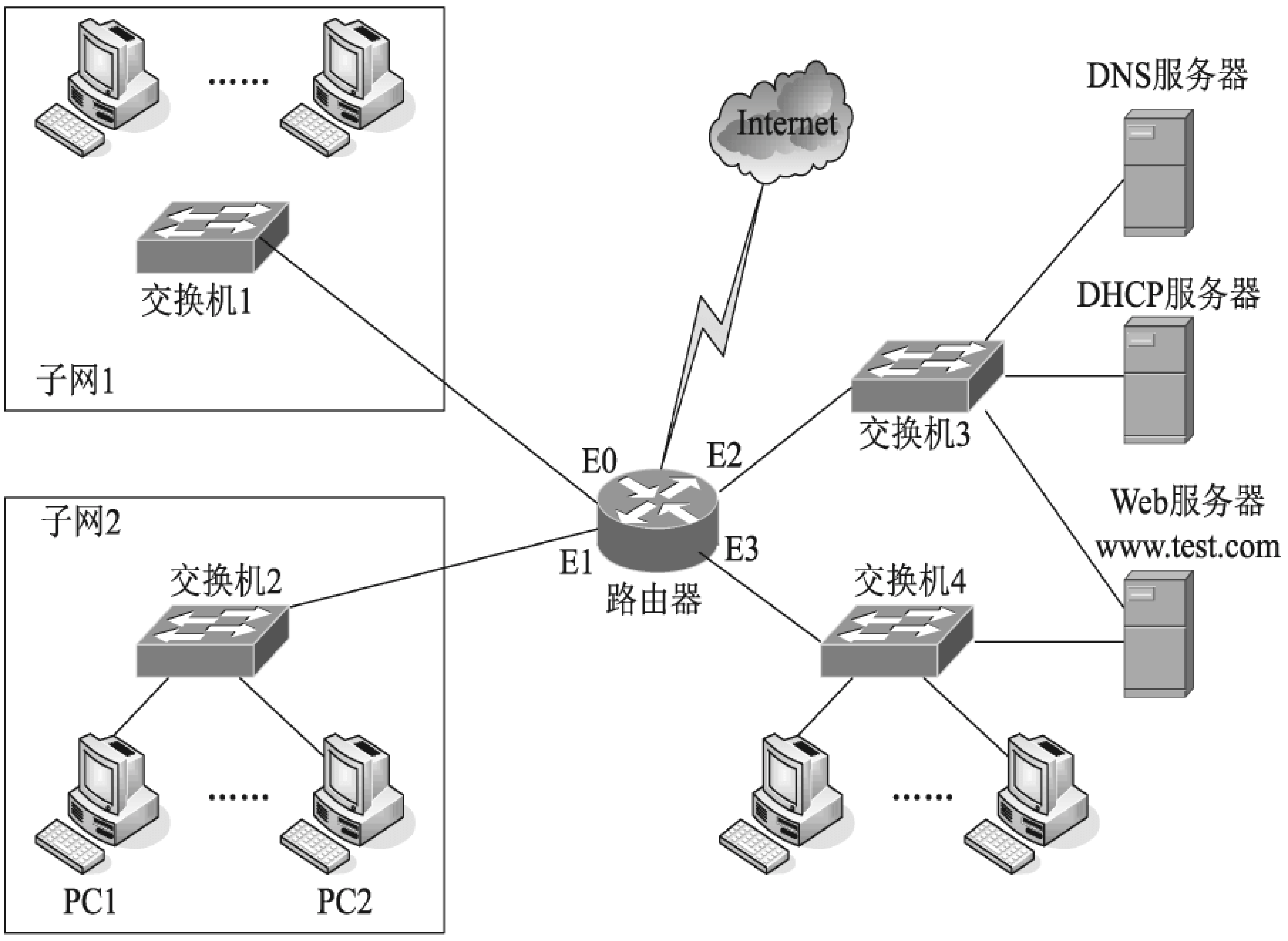


图 5-6　网络拓扑结构图

【问题 1】(3 分)

请完成图 5-6 中 Web 服务器 eth1 的配置。

```
Device=eth1
Bootproto=static
Onboot=yes
Hwaddr=08:00:27:24:F8:9B
Netmask=__(1)__
Ipaddr=__(2)__
Gateway=__(3)__
Type=Ethernet
Name="Systemeth1"
Ipv6intt=no
```

【问题 2】

请完成 DNS 服务器上的配置。

```
Device=eth0
Bootproto=static
Onboot=yes
Hwaddr=08:00:27:21:A1:78
Netmask= (4)
Ipaddr= (5)
Gateway= (6)
Type=Ethernet
Name="Systemeth0"
Ipv6intt=no
```

【问题 3】

在(7)、(8)、(9)处填写恰当的内容。在 Linux 系统中设置域名解析服务器，已知域名服务器上文件 named.conf 的部分内容如下：

```
options{
Directory "/var/named";
Hostname "nsl.test.com";
allow-query {any;};
allow-recursion {A:B:C:D};
Recursion yes;
};
acl "A" {192.168.1.0/25};
acl "B" {192.168.1.128/25};
acl "C" {192.168.2.0/29};
acl "D"{192.168.1.32/29};
View "A"{
Match-clients{A;};
Recursion yes;
Zone "test.com"{
Type master;
File "test.com.zone.A"
};
};
View "B"{
Match-clients{any;};
Recursion yes;
Zone "test.com"{
Type master;
File "test.com.zone.B"
};
};
```

test.com.zone.A 文件的部分配置如下：WWW IN A 192.168.2.4。

test.com.zone.B 文件的部分配置如下：WWW IN A 192.168.2.34。

IP 地址__(7)__不允许使用该 DNS 进行递归查询，子网 1 和子网 2 中的客户端访问 www.test.com 时，该 DNS 解析返回的 IP 地址分别为__(8)__和__(9)__。

(7)备选答案：

A. 192.168.1.8　　B. 192.168.2.34

C. 192.168.2.10　　D. 192.168.2.6

(8)和(9)备选答案：

A. 192.168.2.4　　B. 192.168.2.34

C. 192.168.2.4 或者 192.168.2.34　　D. 192.168.2.4 和 192.168.2.34

【问题 4】

DHCP 服务器配置文件如下：

```
Authoritative;
Ddns-update off;
Max-lease-time 604800;
default-lease-time 604800;
Allow unknow-clients;
Option domain-name-servers 192.168.2.2;
Ddns-update-style none;
allow client-update;
subnet 192.168.0.0 netmask 255.255.255.248{
option routers 192.168.2.33;
range 192.168.2.35 192.168.2.38;
}
```

根据这个文件内容，该 DHCP 服务器默认租期__(10)__天。DHCP 客户机能获得的 IP 地址范围是从__(11)__到__(12)__，获得 DNS 服务器 IP 地址为__(13)__。

答案：

【问题 1】

(1) 255.255.255.248　(2) 192.168.2.34　(3) 192.168.2.33

【问题 2】

(4) 255.255.255.248　(5) 192.168.2.2　(6) 192.168.2.1

【问题 3】

(7) C 或 192.168.2.10　(8) A 或 192.168.2.4　(9) B 或 192.168.2.34

【问题 4】

(10) 7　(11) 192.168.2.35　(12) 192.168.2.38　(13) 192.168.2.2

解析：

【问题 1】

题干已经说明 Web 服务器的 eth1 接口 IP 地址为 192.168.2.34，由于该接口与路由器 E3 接口属于一个逻辑网路，所以其子网掩码长度为“/29”，十进制的表示为 255.255.255.248，路由器 E3 接口的 IP 地址 192.168.2.33/29 为 Web 服务器 eth1 接口的网关地址。

【问题 2】

本问题考查网络地址规划和 Linux 系统下网卡网络配置的基本知识和两种表示方式的子网掩码换算。

Linux 系统下网络配置参数中，NETMASK 代表子网掩码，IPADDR 代表 IP 地址，GATEWAY 代表子网网关地址。

【问题 3】

本问题考查 Linux 系统下基于 BIND 的 DNS 服务配置。

通过 allow-recursion{A;B;C;D}命令，可以看出 acl A、B、C、D 允许递归查询，选项 A、B、D 对应的 IP 地址分别在定义的 acl A、B、C 子网中，选项 C 对应的 IP 地址不在 acl A、B、C、D 任何子网中，故选 C。

客户端访问 www.test.com 时，子网 1 的客户端对应 acl A，会访问 view A 中的域名配置文件 test.com.zone.A，故解析出的 IP 地址为 192.168.2.4; 子网 2 的客户端不在 acl A 中，则会访问 view B 中的域名配置文件 test.com.zone.B，故解析出的 IP 地址为 192.168.2.34。

【问题 4】

通过 DHCP 服务器配置命令中“default-lease-time 604800”语句分析，默认租约时间为 604800 秒，亦即 7 天。通过语句“option domain-name-servers 192.168.2.2”，可以得到 DHCP 服务器获得的 DNS IP 地址为 192.168.2.2。通过语句“range 192.168.2.35 192.168.2.38”，可以得到 DHCP 客户能获得的 IP 地址范围是 192.168.2.35～192.168.2.38。

5.2.3 同步练习

阅读以下 Linux 系统中关于 IP 地址和主机名转换的说明，回答问题 1 至问题 3。

【说明】 计算机用户通常使用主机名来访问网络中的节点，而采用 TCP/IP 协议的网络是以 IP 地址来标记网络节点的，因此需要一种将主机名转换为 IP 地址的机制。在 Linux 系统中，可以使用多种技术来实现主机名和 IP 地址的转换。

【问题 1】(6 分)

请选择恰当的内容填写在(1)～(3)空白处。

一般用 Host 表、网络信息服务系统(NIS)和域名服务(DNS)等多种技术来实现主机名和 IP 地址之间的转换。Host 表是简单的文本文件，而 DNS 是应用最广泛的主机名和 IP 地址的转换机制，它使用__(1)__来处理网络中成千上万个主机和 IP 地址的转换。在 Linux 中，DNS 是由 BIND 软件来实现的。BIND 是一个__(2)__系统，其中的 resolver 程序负责产生域名信息的查询，一个称为__(3)__的守护进程，负责回答查询，这个过程称为域名解析。

(1) A. 集中式数据库　　B. 分布式数据库

(2) A. C/S　　B. B/S

(3) A. named　　B. bind　　C. nameserver

【问题 2】(3 分)

图 5-7 是采用 DNS 将主机名解析成一个 IP 地址过程的流程图。请选择恰当的内容填写在(4)～(6)空白处。

A. 产生一个指定下一域名服务器的响应，送给 DNS 客户

B. 把名字请求转送给下一个域名服务器，进行递归求解，结果返回给 DNS 客户

C. 将查询报文发往某域名服务器

D. 利用 Host 表查询

E. 查询失败

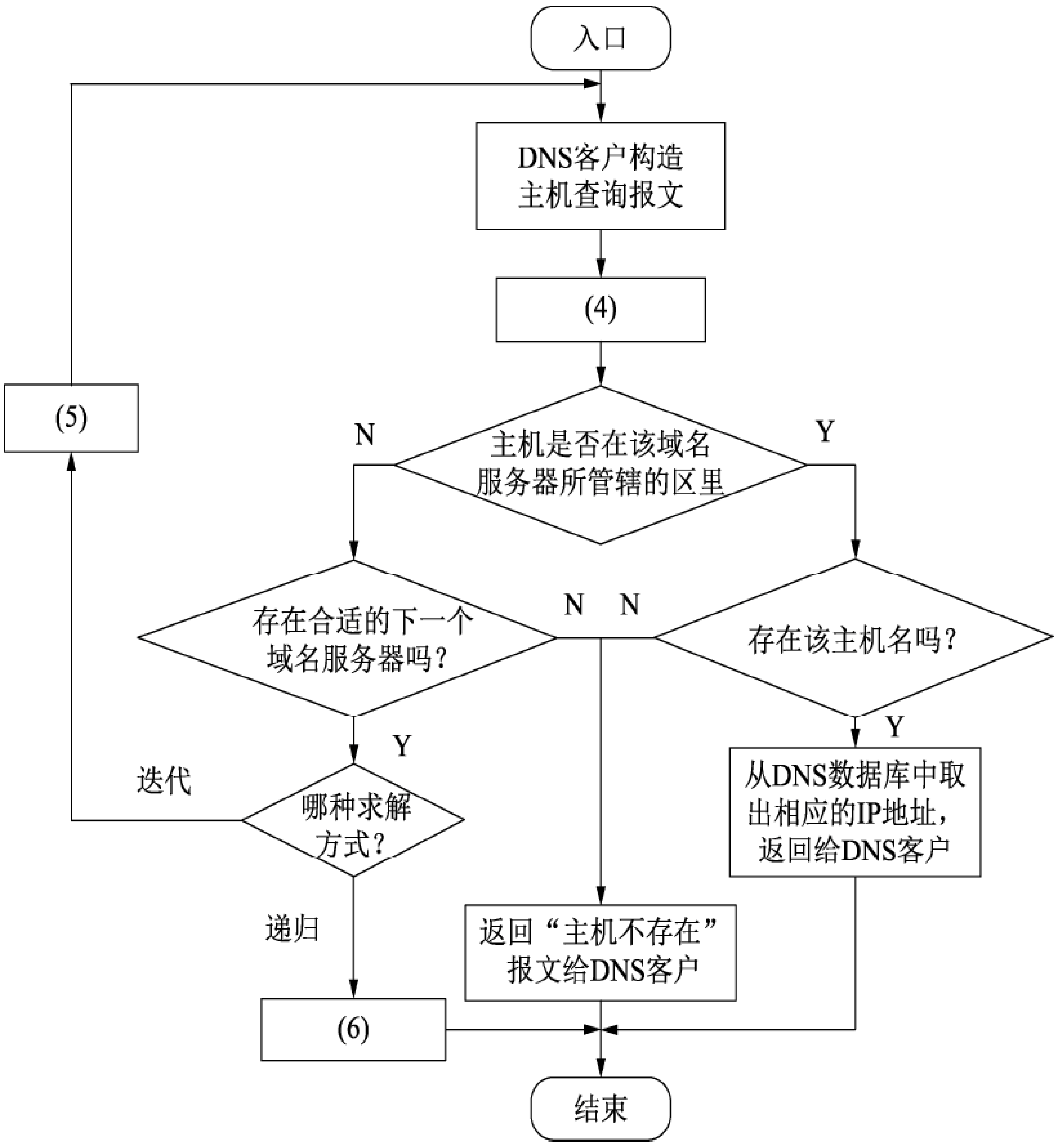


图 5-7　DNS 解析流程图

【问题 3】(6 分)

请在(7)～(9)空白处填写恰当的内容。

在 Linux 系统中设置域名解析服务器，已知该域名服务器上文件 named.conf 的部分内容如下。

```
options {
       directory '/var/named';
  };
  zone '.' {
      type hint;
      file 'named.ca';
  }
  zone 'localhost' IN {
      file "localhost.zone"
      allow-update{none;};
  };
  zone '0.0.127.in-addr.arpa'{
      type master;
      file 'named.local';
  };
  zone 'test.com'{
      type  (7) ;
      file 'test.com';
  };
```

```
zone '40.35.222.in-addr.arpa'{
    type master;
    file '40.35.222';
};
include "/etc/rndc.key";
```

该服务器是域 test.com 的主服务器，该域对应的网络地址是 (8) ，正向域名转换数据文件存放在 (9) 目录中。

5.2.4 同步练习参考答案

答案：

【问题 1】

(1) B　(2) A　(3) A

【问题 2】

(4) C　(5) A　(6) B

【问题 3】

(7) master　(8) 222.35.40.0　(9) /var/named

5.3 DHCP 服务器的配置

5.3.1 考点辅导

在 Linux 操作系统下建立 DHCP 服务器非常简单，只要掌握几个简单的命令，编辑 /etc/dhcpd.conf 文件，就能够很快建立 DHCP 服务器。

5.3.1.1 DHCP 的常用概念

1. 作用域

作用域是一个网络中可分配 IP 地址的集合。

2. 超级作用域

超级作用域是一组作用域的集合，是由一个物理子网中包含的多个 IP 子网组成的。我们可以理解为作用域是一个用户，而超级作用域就是这个用户的组。

3. 排除范围

排除范围是用来定义某 IP 或者某一组 IP 不出现在 DHCP 作用域中。

4. 地址池

定义了 DHCP 作用域和排除范围后，剩下的可用地址构成了一个地址池。池中的地址可以分配给用户使用。

5. 租约

租约就是 DHCP 服务器指定的时间长度，在此长度内客户机可以使用分配给它的地址，如果租约到期，客户机必须更新 IP 租约。

6. 保留地址

用户可以使用保留地址，保留地址提供了一个将动态地址和其 MAC 地址相关联的手段，用于保证此网卡长期使用某个 IP 地址。

7. 选项类型

选项类型是 DCHP 为工作站提供的其他参数，比如网关的 IP 地址、DNS 服务器等。

5.3.1.2　DHCP 的设置

DHCP 的配置文件是/etc/dhcpd.conf，不过默认情况下这个文件不存在，需要使用它的模板建立一个配置文件。模板的位置在/usr/share/doc/dhcp-3.0p11/dhcpd.conf.sample 中。

模板配置文件的内容如下。

和所有的配置文件类似，它用#代表注释。现在看看每行都说了什么。

```
ddns-update-style interim;
#配置使用过渡性 DHCP-DNS 互动更新模式
ignore client-updates;
#忽略客户端更新
subnet 192.168.0.0 netmask 255.255.255.0 {
#设置子网声明
# --- default gateway
option routers 192.168.0.1;
#设置默认网关为 192.168.0.1

option subnet-mask 255.255.255.0;
#设置客户端的子网掩码
option nis-domain "domain.org";
#为客户设置 NIS 域
option domain-name "domain.org";
#为客户设置域名
option domain-name-servers 192.168.1.1;
#为客户设置域名服务器
option time-offset -18000; # Eastern Standard Time
#设置偏移时间
# option ntp-servers 192.168.1.1;
设置 NTP 服务器
# option netbios-name-servers 192.168.1.1;
设置 WINS 服务器
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
# option netbios-node-type 2;
#设置 netbios 节点类型
```

```
range dynamic-bootp 192.168.0.128 192.168.0.255;
#设置动态的地址池
default-lease-time 21600;
#设置默认的地址租期

max-lease-time 43200;
#设置客户端最长的地址租期

# we want the nameserver to appear at a fixed address
//设置主机声明
host ns {
next-server marvin.redhat.com;
//设置定义服务器从引导文件中装入的主机名，用于无盘站
hardware ethernet 12:34:56:78:AB:CD;
//指定 DHCP 客户的 MAC 地址
fixed-address 207.175.42.254;
//给指定的 MAC 地址分配 IP
}
}
```

5.3.2　典型例题分析

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【问题 1】(3 分，每空 1.5 分)

Linux 服务器中 DHCP 服务程序/usr/sbin/dhcpd 对应的配置文件名称是__(1)__，该文件的默认目录是__(2)__。

【问题 2】(6 分，每空 1 分)

某网络采用 Linux DHCP 服务器为主机提供服务，查看某主机的网络连接详细信息如图 5-8 所示。

图 5-8　网络连接详细信息

请根据图 5-8 补充完成 Linux DHCP 服务器中 DHCP 配置文件的相关配置项。

```
subnet 192.168.1.0   netmask 255.255.255.0
{range 192.168.1.10 192.168.1.200;default-lease-time  (3) ;
max-lease-time  14400;
option subnet-mask  (4) ;
option routers  (5) v
option domain-name "myuniversity.edu.cn";option broadcast-address  (6) ;
option domain-name-servers  (7) ,  (8) ;}
```

【问题 3】(6 分，每空 2 分)

如果要确保 IP 地址 192.168.1.102 分配给图 5-8 中的 PC，需要在 DHCP 配置文件中补充以下语句。

```
 (9)  pcl{hardware ethernet  (10)  ;fixed-address  (11)  ;}
```

答案：

【问题 1】

(1) dhcpd.conf (2) /etc

【问题 2】

(3) 7200 (4) 255.255.255.0 (5) 192.168.1.1 (6) 192.168.1.255

(7) 218.30.19.50 (8) 61.134.1.4

【问题 3】

(9) host (10) 00:24:D2:DF:37:F3 (11) 192.168.1.102

解析：

【问题 1】DHCP 服务的守护程序是/usr/sbin/dhcpd。默认的配置文件是/etc/dhcpd.conf。

【问题 2】 由图 5-8 可知，获得租约的时间是 2012-2-10 20:51:53，租约过期的时间是 2012-2-10 22:51:53，故默认租用期为 2 小时，即 7200 秒，故(3)处填 7200; (4)处填子网掩码，即 255.255.255.0; option routers 指明子网内的默认网关(即路由器)的地址，故(5)处填默认网关 192.168.1.1; option broadcast-address 指定广播地址，即将 IP 地址的网络号都置为 1，故(6)处填 192.168.1.255; option domain-name-servers 指定 DNS 服务器，可以有多个，故(7)、(8)处分别填 218.30.19.50 和 61.134.1.4。

【问题 3】 fixed-address 指定一个或多个 IP 地址给一个 DHCP 客户，只能出现在 host 声明里，故(9)处填 host，(10)处填以太网的 MAC 地址，图 5-8 中所示为 00:24:D2:DF:37:F3，(11)处填固定的 IP 地址 192.168.1.102。

5.3.3 同步练习

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】 在大型网络中，通常采用 DHCP 完成基本网络配置会更有效率。

【问题 1】(1 分)

在 Linux 系统中，DHCP 服务默认的配置文件为 (1) 。

(1)备选答案：

A. /etc/dhcpd.conf　　B. /etc/dhcpd.config

C. /etc/dhcp.conf　　D. /etc/dhcp.config

【问题 2】(4 分)

管理员可以在命令行中通过 (2) 命令启动 DHCP 服务；通过 (3) 命令停止 DHCP 服务。

(2)、(3)备选答案：

A. service dhcpd start　　B. service dhcpd up

C. service dhcpd stop　　D. service dhcpd down

【问题 3】(10 分)

在 Linux 系统中配置 DHCP 服务器，该服务器配置文件的部分内容如下。

```
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers    192.168.1.254;
option subnet-mask   255.255.255.0;
option broadcast-address  192.168.1.255;
option domain-name-servers 192.168.1.3;
range 192.168.1.100 192.168.1.200;
default-lease-time  21600;
max-lease-time  43200;
host webserver{
hardware ethernet 52:54:AB:34:5B:09;
fixed-address  192.168.1.100;
  }
}
```

在主机 Web Server 上运行 ifconfig 命令时显示如下，根据 DHCP 配置，填写空格中缺少的内容。

```
eth0      Link encap:Ethernet  HWaddr  (4)
          inet addr:  (5)    Bcast:192.168.1.255   Mask:  (6)
          UP BROADCAST RUNNING MULTICAST   MTU:1500   Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)   TX bytes:168 (168.0 b)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1   Mask:255.0.0.0
          UP LOOPBACK RUNNING   MTU:16436   Metric:1
          RX packets:397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:397 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26682 (26.0 Kb)   TX bytes:26682 (26.0 Kb)
```

该网段的网关 IP 地址为 (7) ，域名服务器的 IP 地址为 (8) 。

5.3.4　同步练习参考答案

答案：

【问题 1】

(1) A

【问题 2】

(2) A　　(3) C

【问题 3】

(4) 52:54:AB:34:5B:09　　(5) 192.168.1.100　　(6) 255.255.255.0

(7) 192.168.1.254　　(8) 192.168.1.3

5.4　Samba 服务器的配置

5.4.1　考点辅导

Samba 能够使 Windows 用户通过“网上邻居”等熟悉的方式直接访问 Linux 上的资源，也能使 Linux 利用 SMB 客户端程序访问 Windows 的共享资源。

服务信息块(Server Message Block，SMB)是局域网上的共享文件夹/打印机的一种协议。

Samba 的配置文件如下。

```
 [global]
  workgroup = WORKGROUP
   server string = Samba Server
   printcap name = /etc/printcap
   load printers = yes
cups options = raw
log file = /var/log/samba/%m.log
   max log size = 50
   security = user
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   dns proxy = no
   idmap uid = 16777216-33554431
   idmap gid = 16777216-33554431
   template shell = /bin/false
   winbind use default domain = no
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
[printers]
```

```
comment = All Printers
path = /var/spool/samba
browseable = no
guest ok = no
writable = no
printable = yes
```

从上面的程序中可以看到 Samba 的配置文件分为三节。

[global]：这个小节主要包含全局参数。

[homes]：这个小节用于共享存储在\home 中的 Linux 用户目录。

[printers]：这个小节用于共享本地 Linux 打印机文件/etc/printcap 中列出的所有打印机。

1. [global] 全局参数配置

[global] 全局参数配置命令如下。

```
workgroup = WORKGROUP
netbios = dolinux.cn
server string = NetSeek's Samba Server(%h Samba Server)
hosts allow = netseek,cnseek.org,192.168.0.*EXPECT 192.168.0.5
//允许主机名为netseek 的客户端访问，允许域为 cnseek.org 的域访问，允许 192.168.0.*
//所有的主机访问，除了 192.168.0.5
 printcap name = /etc/printcap
//Samba 启动时，将会自动加载打印机配置文件，建议默认即可
 load printers = yes            //允许自动加载浏览列表，默认即可
log file = /var/log/samba/%m.log  //samba 相关的日志文件
security = user   //使用的安全等级，默认值为 user
```

其安全等级分为以下 5 类。

(1) share：当客户端连接到该等级的 Samba 服务器上时，不需要输入账号和密码，就可以访问 Samba 服务器上的共享资源，但安全性无法保证。

(2) user：用户需要输入有效的密码，通过验证后才能使用服务器的共享。

(3) server：与 user 等级相同，也需要输入有效的账号和密码，但还需要指定口令服务器。其配置命令如下。

```
password server =  <NT-Server-Name>
eg: security = server
password server= SMB2
smb passwd file =/etc/samba/smbpasswd_smb2
```

(4) domain 安全等级：Samba 服务器加入到 Windows NT 域中后，Samba 的服务器不再负责账号和密码的验证，而是统一由域控制器负责，此时需要使用访问安全等级，同时也必须指定口令服务器。

(5) ads 安全等级：Samba 服务器加入到 Windows 活动目录后，需要使用访问安全等级，同时也需要指定口令服务器。其配置命令如下。

```
password level = 8
```

```
username level = 8          //用户名和密码长度限制
encrypt passwords = yes     //使用口令加密
smb passwd file = /etc/samba/smbpasswd
//Smaba 账号存放文件，注意务必采用加密形式，否则要改 win 注册表，因为 win 也采用了加密方式
username map = /etc/samba/smbusers //用户映射，将不同的用户映射成为一个用户
```

2. [homes] 设置共享目录

[homes]设置共享目录的配置命令如下。

```
[homes]
 comment = Home Directories//目录文字说明
browseable = no             //是否允许用户浏览 homes 主目录，建议使用默认值不允许
writable = yes              //是否允许写入个人主目录
comment = 文字说明内容       //文字说明
browseable = no //表示禁止浏览，也就是本目录只有有权使用的用户可以看到
writable = yes //允许有权限的用户写入
valid users = netseek,lin,@share //只允许 netseek、lin、用户 share 组的访问
```

设置一个共享目录的命令如下。

```
[shares]
comment = NetSeek's share Directory
read list = netseek
write list = @share
path = /home/share
```

【说明】NetSeek 的用户可以读，share 组的用户可以读写，所有 share 的用户对这个目录可读可写。

3. [printers] 共享打印

[printers] 共享打印的配置命令如下。

```
   comment = All Printers
   path = /var/spool/samba
   browseable = no
   //如果允许 guest 打印，只需在末尾加入 public = yes 即可
   # Set public = yes to allow user 'guest account' to print
   guest ok = no
   writable = no
   printable = yes
```

4. 用户创建

(1) 系统用户映射给 Samba，其配置命令如下。

```
#cat /etc/passwd | /usr/bin/mksmbpasswd.sh > /etc/samba/smbpasswd
```

(2) 为用户添加 SMB 口令，其配置命令如下。

```
#smbpasswd netseek
New SMB password:*******
Retype new SMB password:*******
```

5. 服务启动

服务启动的命令如下。

```
/etc/rc.d/init.d/smb start
/etc/rc.d/init.d/smb restart
#chkconfig smb on
#chkconfig --list smb
```

5.4.2 典型例题分析

阅读以下关于 Linux 文件系统和 Samba 服务的说明，回答问题 1 至问题 3。

【说明】 Linux 系统采用了树型多级目录来管理文件，树型结构的最上层是根目录，其他的所有目录都是从根目录生成的。

通过 Samba 可以实现基于 Linux 操作系统的服务器和基于 Windows 操作系统的客户机之间的文件、目录及共享打印服务。

【问题 1】(6 分)

Linux 在安装时会创建一些默认的目录，如表 5-1 所示。

表 5-1 Linux 的默认目录

目 录	说 明
/	
/bin	
/boot	存放启动系统使用的文件
/dev	
/etc	用来存放系统管理所需要的配置文件和子目录
/home	
/lib	文件系统中程序所需要的共享库
/lost+found	
/mot	临时安装(mount)文件系统的挂载点
/opt	
/proc	
/root	
/sbin	
/usr	
/var	包含系统运行时要改变的数据
/tmp	

依据上述表格，在空(1)～(6)中填写恰当的内容[其中空(1)在备选答案中选择]。

1. 对于多分区的 Linux 系统，文件目录树的数目是 (1) 。

2. Linux 系统的根目录是 (2) ，默认的用户主目录在 (3) 目录下，系统的设备文件(如打印驱动)存放在 (4) 目录中， (5) 目录中的内容关机后不能被保存。

3. 如果在工作期间突然停电，或者没有正常关机，在重新启动机器时，系统将要复查文件系统，系统将找到的无法确定位置的文件放到目录 (6) 中。

(1)备选答案：

A. 1　　　　B. 分区的数目　　　　C. 大于 1

【问题 2】(4 分)

默认情况下，系统将创建的普通文件的权限设置为-rw-r--r--，即文件所有者对文件 (7) ，同组用户对文件 (8) ，其他用户对文件 (9) ，文件的所有者或者超级用户，采用 (10) 命令可以改变文件的访问权限。

【问题 3】(5 分)

Linux 系统中 Samba 的主要配置文件是/etc/samba/smb/conf，请根据以下的 smb.conf 配置文件，在空(11)～(15)中填写恰当的内容。

Linux 服务器启动 Samba 服务后，在客户机的“网上邻居”中显示提供共享服务的 Linux 主机名为 (11) ，其共享的服务有 (12) ，能够访问 Samba 共享服务的客户机的地址范围是 (13) ；能够通过 Samba 服务读写/home/samba 中内容的用户是 (14) ；该 Samba 服务器的安全级别是 (15) 。

```
[global]
workgroup = MYGROUP
netbios name = smb-server
server string = Samba Server
hosts allow = 192.168.1 192.168.2.127
load printers =yes

[printers]
comment = My Printer
browseable = yes
path = /usr/spool/samba
guest ok = yes
writable = no
printable = yes

[public]
comment = Public Test
browseable = no
path = /home/samba
public = yes
writable = yes
printable = no
write list = @test

[user 1 dir]
comment = Userl's Service
browseable = no
path = /usr/usrl
valid uers = userl
public = no
writable = yes
printable = no
```

答案：

【问题 1】

(1) A　(2) /　(3) /home　(4) /dev　(5) /proc　(6) /lost+found

【问题 2】

(7) 可读可写不可执行　(8) 可读不可写不可执行

(9) 可读不可写不可执行　(10) chmod

【问题 3】

(11) smb-server　(12) (printers 或 My Printer)文件及打印共享

(13) 因为相关参数被注释，因此没有范围限制

(14) test 用户组　(15) user

解析：

【问题 1】 Linux 系统中的每个分区都是一个文件系统，都有自己的目录层次结构。Linux 将这些属于不同分区的、单独的文件系统按照挂载的方式，将一个文件系统的顶层目录挂到另一个文件系统的子目录上，形成一个系统的树型层次结构。树型结构的最上层是根目录，用“/”表示，其他的目录都是从根目录出发而生成的。/home 目录下存放的是用户文件的主目录，用户数据存放在其主目录中；/dev 目录下存放的是设备文件；/proc 是一个虚拟的文件系统(不是实际储存在磁盘上的)，是由系统启动的时候在内存中产生的，存放存储进程和系统信息，其内容在关机后不能被保存；/lost+found 目录在大多数情况下都是空的，但当突然停电或者非正常关机后，在机器启动的时候有些文件找不到应该存放的地方，就放到这个目录中。

【问题 2】Linux 对文件的访问设定了 3 级权限：文件所有者、文件所有者同组的用户和其他用户。它对文件的访问设定了 3 种处理操作：读取、写入和执行。每一个文件或目录的列表信息分为 4 部分，其中最左边的一位标识操作系统的文件类型，其余 3 组是 3 组访问权限，每组用 3 位表示，r 表示可读的，w 表示可写的，x 表示可执行的，-表示无访问权限。题目中文件的权限设置为-rw-r--r--，则文件所有者对该文件可读可写(rw)，而同组用户和其他用户对该文件只可读(r)。

chmod 命令用于改变文件或目录的访问权限。用户根据需要可以通过命令修改文件和目录的默认存取权限，只有文件所有者或者超级用户才有权用 chmod 改变文件或目录的访问权限。

【问题 3】 下面是 Samba 主要配置文件的说明，与所有的配置文件类似，它用#代表注释。

```
    [global]
    workgroup = MYGROUP
#PDC 域
    netbios name = smb-server
#在其他的机器中声明的本机器的名称
    server string = Samba Server
#这个声明会出现在 Windows 的“网上邻居”中
    hosts allow = 192.168.1 192.168.2.127
#这一行由于安全的原因很关键，只许在局域网中与特定的计算机连接
```

```
load printers = yes
#自动载入一个打印机的清单

    [printers]
   comment = My Printer
   browseable = yes
   path = /usr/spool/samba
   guest ok = yes
   writable = no
   printable = yes

    [public]
   comment = Public Test
#文字说明内容
   browseable = no
#表示禁止浏览，也就是本目录只允许有权使用的用户可以看到
   path = /home/samba
#设置共享的路径
   public = yes
   writable = yes
   printable = no
   write list = @test

    [user 1 dir]
   comment = Userl's Service
#文字说明内容
   browseable = no
#表示禁止浏览，也就是本目录只允许有权使用的用户可以看到
   path = /usr/usrl
#设置共享的路径
   valid uers = userl
#指定可访问的用户
   public = no
   writable = yes
#允许有权限的用户写入
   printable = no
```

5.4.3　同步练习

阅读以下说明，回答问题 1 至问题 8，将解答填入答题纸对应的解答栏内。

【说明】 Linux 系统开机引导时首先启动内核，由内核检查和初始化硬件设备，载入设备的驱动程序模块，安装 root 文件系统，然后内核将启动一个名为 init 的进程。在 init 运行完成并启动其他必要的后续进程后，系统开始运行，引导过程结束。init 进程启动时需要读取 inittab 配置文件，该文件确定 init 在系统启动和关机时的工作特性。典型的 inittab 文件内容见以下清单。

```
#
# inittab   This file describes how the INIT process should set up
#   '      the system in a certain run-level.
#

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:5:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

【问题 1】(2 分)

启动 init 进程前，不需要经过__(1)__步骤。

A. LILO 加载内核　　B. 检测内存

C. 加载文件系统　　D. 启动网络支持

【问题 2】(2 分)

inittab 文件存放在__(2)__目录中。

A. /etc　　B. /boot　　C. /sbin　　D. /root

【问题 3】(2 分)

Linix 系统运行级别 3 工作在__(3)__状态。

A. 单用户字符模式　　B. 多用户字符模式

C. 单用户图形模式　　D. 多用户图形模式

【问题 4】(2 分)

根据说明中 inittab 文件的内容，系统引导成功后，工作在__(4)__状态。

A. 单用户字符模式　　B. 多用户字符模式

C. 单用户图形模式　　D. 多用户图形模式

【问题 5】(2 分)

在系统控制台，__(5)__用 Ctrl+Alt+Delete 组合键来重新引导服务器。

A. 允许　　B. 不允许

【问题 6】(2 分)

假设 root 用户执行 init 0 命令，系统将会__(6)__。

A. 暂停　　B. 关机　　C. 重新启动　　B. 初始化

【问题 7】(2 分)

root 用户执行 ps aux | grep init 命令，得到 init 的 PID 是__(7)__。

A. 0　　B. 1　　C. 2　　D. 3

【问题 8】(1 分)

根据上述 inittab 文件的内容，系统在引导过程结束前，至少还要执行__(8)__进程。

A. rc.sysinit

B. rc.sysinit 和 rc 5

C. rc.sysinit、rc 0、rc 1、rc 2、rc 3、rc 4、rc 5 和 rc 6

D. rc 0、rc 1、rc 2、rc 3、rc 4、rc 5 和 rc 6

5.4.4　同步练习参考答案

答案：

【问题 1】D

【问题 2】A

【问题 3】B

【问题 4】D

【问题 5】A

【问题 6】B

【问题 7】B

【问题 8】B

5.5 本章小结

本章知识点在 2014 年的新大纲中变化不大，只是要求更加明细化，并在表述方式上做了一些调整。

本章主要要求考生掌握 Linux 网络服务的基本功能以及相关服务器的配置，包括 Apache、DNS、DHCP 和 Samba 服务器的配置。

本章内容为下午科目的重点内容，为每次考试必考的内容。希望考生针对相应的知识点，全面掌握 Linux 网络服务的相关内容。本章的每小节针对考试大纲，组织了近 5 年来的真题和小部分模拟题，这些题目将有助于考生理解和掌握大纲中的知识点。

第6章 网 络 安 全

大纲要求：

- 访问控制与防火墙，包括 ACL 命令、过滤规则和防火墙配置。
- 数字证书。
- VPN 配置。
- PGP。
- 病毒防护。

6.1 防火墙配置

6.1.1 考点辅导

6.1.1.1 防火墙介绍

任何企业安全策略的一个主要部分都是实现和维护防火墙，因此防火墙在网络安全的实现中扮演着重要的角色。防火墙通常位于企业网络的边缘，这使得内部网络与 Internet 或者其他外部网络互相隔离，并限制网络互访从而保护企业内部网络。设置防火墙的目的都是在内部网与外部网之间设立唯一的通道，简化网络的安全管理。

在众多的企业级主流防火墙中，Cisco PIX 防火墙是所有同类产品中性能最好的一种。Cisco PIX 系列防火墙目前有 5 种型号：PIX506、515、520、525 和 535。这里将以 PIX525 为例介绍防火墙的配置。

6.1.1.2 防火墙的物理特性

在配置 PIX 防火墙之前，先来介绍一下防火墙的物理特性。防火墙通常至少具有 3 个接口，但许多早期的防火墙只具有 2 个接口。当使用具有 3 个接口的防火墙时，会产生至少 3 个网络，它们的描述如下。

1. 内部区域(内网)

内部区域通常就是指企业内部网络或者企业内部网络的一部分。它是互联网(Interconnection Network)的信任区域，即受到了防火墙的保护。

2. 外部区域(外网)

外部区域通常指 Internet 或者非企业内部网络。它是互联网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务时，通过设置防火墙就可以实现有限制的访问。

3. 非军事区(DMZ)

非军事区是一个隔离的网络，或几个网络。位于非军事区中的主机或服务器被称为堡

垒主机。一般在非军事区内可以放置 Web 服务器和 E-mail 服务器等。非军事区对于外部用户通常是可以访问的，这种方式允许外部用户访问企业的公开信息，但却不允许他们访问企业内部网络。

6.1.1.3 防火墙管理模式

PIX 防火墙提供以下 4 种管理访问模式。

1. 非特权模式

PIX 防火墙开机自检后，就是处于这种模式。系统显示为 pixfirewall> 。

2. 特权模式

输入 enable 命令即进入特权模式，可以改变当前配置。系统显示为 pixfirewall# 。

3. 配置模式

输入 configure terminal 命令即进入配置模式，绝大部分的系统配置都在这里进行。系统显示为 pixfirewall(config)# 。

4. 监视模式

PIX 防火墙在开机或重启过程中，按住 Esc 键或发送一个“Break”字符，可以进入监视模式。在这里可以更新操作系统映像和口令恢复。系统显示为 monitor>。

6.1.1.4 PIX 防火墙基本命令

下面介绍配置 PIX 防火墙的 6 个基本命令：nameif、interface、ip address、nat、global 和 route。

1. 配置防火墙接口的名字，并指定安全级别(nameif)

```
Pix525(config)#nameif ethernet0 outside security 0
Pix525(config)#nameif ethernet1 inside security 100
Pix525(config)#nameif dmz security 50
```

提示：在默认配置中，以太网 0 被命名为外部接口(outside)，安全级别是 0；以太网 1 被命名为内部接口(inside)，安全级别是 100。安全级别的取值范围为 1～99，数字越大安全级别越高。若添加新的接口，语句如下所示。

```
Pix525(config)#nameif pix/intf3 security 40 (安全级别任取)
```

2. 配置以太口参数(interface)

```
Pix525(config)#interface ethernet0 auto(auto 选项表明系统自适应网卡类型)
Pix525(config)#interface ethernet1 100full(100full 选项表示 100 Mbps 以太网全双工通信)
Pix525(config)#interface ethernet1 100full shutdown (shutdown 选项表示关闭这个接口，若启用接口则去掉 shutdown)
```

3. 配置内外网卡的 IP 地址(ip address)

```
Pix525(config)#ip address outside 61.144.51.42 255.255.255.248
```

```
Pix525(config)#ip address inside 192.168.0.1 255.255.255.0
```

提示：PIX525 防火墙在外网的 IP 地址是 61.144.51.42，内网的 IP 地址是 192.168.0.1。

4. 指定要进行转换的内部地址(nat)

网络地址翻译(nat)的作用是将内网的私有 IP 转换为外网的公有 IP。nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

nat 命令的配置语法如下：

```
nat (if_name) nat_id local_ip
```

其中(if_name)表示内网接口名字；nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配；local_ip 表示内网被分配的 IP 地址。例如 0.0.0.0 表示内网所有主机可以对外访问。

例 1

```
Pix525(config)#nat (inside) 1 0 0
```

表示启用 nat，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0。

例 2

```
Pix525(config)#nat (inside) 1 172.16.5.0 255.255.0.0
```

表示只有 172.16.5.0 这个网段内的主机可以访问外网。

5. 指定外部地址范围(global)

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。

global 命令的配置语法如下：

```
global (if_name) nat_id ip_address-ip_address
```

其中(if_name)表示外网接口名字；nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配；ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址的范围。

例 1

```
Pix525(config)#global (outside) 1 61.144.51.42-61.144.51.48
```

表示内网的主机通过 PIX 防火墙要访问外网时，PIX 防火墙将使用 61.144.51.42- 61.144.51.48 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

例 2

```
Pix525(config)#global (outside) 1 61.144.51.42
```

表示内网要访问外网时，PIX 防火墙将为访问外网的所有主机统一使用 61.144.51.42 这个单一 IP 地址。

例 3

```
Pix525(config)#no global (outside) 1 61.144.51.42
```

表示删除这个全局表项。

6. 设置指向内网和外网的静态路由(route)

route 命令用来定义一条静态路由。

route 命令的配置语法如下：

```
route (if_name) 0 0 gateway_ip  number
```

其中(if_name)表示接口名字，例如 inside 和 outside；gateway_ip 表示网关路由器的 IP 地址；number 表示到 gateway_ip 的跳数，通常默认是 1。

例 1

```
Pix525(config)#route outside 0 0 61.144.51.168 1
```

表示一条指向边界路由器(IP 地址为 61.144.51.168)的默认路由。

例 2

```
Pix525(config)#route inside 10.1.1.0 255.255.255.0 172.16.0.1 1
Pix525(config)#route inside 10.2.0.0 255.255.0.0 172.16.0.1 1
```

如果内部网络只有一个网段，按照例 1 那样设置一条默认路由即可；如果内部存在多个网络，就需要配置一条以上的静态路由。例 2 表示创建了一条到网络 10.1.1.0 的静态路由，静态路由的下一条路由器 IP 地址是 172.16.0.1。

6.1.1.5 PIX 防火墙高级配置

1. 配置静态 IP 地址翻译(static)

如果从外网发起一个会话，会话的目的地址是一个内网的 IP 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。

static 命令的配置语法如下：

```
static (internal_if_name, external_if_name) outside_ip_address inside_
ip_address
```

其中，internal_if_name 表示内部网络接口，安全级别较高，如 inside。

external_if_name 为外部网络接口，安全级别较低，如 outside 等。

outside_ip_address 为正在访问的较低安全级别接口上的 IP 地址。

inside_ ip_address 为内部网络的本地 IP 地址。

例 1

```
Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.8
```

表示 IP 地址为 192.168.0.8 的主机，对于通过 PIX 防火墙建立的每个会话，都被翻译成 61.144.51.62 这个全局地址，也可以理解成 static 命令创建了内部 IP 地址 192.168.0.8 和外部 IP 地址 61.144.51.62 之间的静态映射。

例 2

```
Pix525(config)#static (inside, outside) 192.168.0.2 10.0.1.3
```

表示创建了内部 IP 地址 192.168.0.8 和外部 IP 地址 10.0.1.3 之间的静态映射。

例 3

```
Pix525(config)#static (dmz, outside) 211.48.16.2 172.16.10.8
```

表示创建了 DMZ 的 IP 地址 211.48.16.2 和外部 IP 地址 172.16.10.8 之间的静态映射。

以上几个例子说明使用 static 命令可以让我们为一个特定的内部 IP 地址设置一个永久的全局 IP 地址。这样就能够为具有较低安全级别的指定接口创建一个入口，使它们可以进入到具有较高安全级别的指定接口。

2. 管道命令(conduit)

前面讲过使用 static 命令可以在一个本地 IP 地址和一个全局 IP 地址之间创建一个静态映射，但从外部到内部接口的连接仍然会被 PIX 防火墙的自适应安全算法(ASA)阻挡。conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，例如允许从外部到 DMZ 或内部接口的入口方向的会话。对于向内部接口的连接，static 和 conduit 命令将一起使用，来指定会话的建立。

conduit 命令的配置语法如下。

```
conduit permit | deny global_ip port<-port> protocol foreign_ip
```

其中，permit | deny 表示允许或拒绝访问。

global_ip 指的是先前由 global 或 static 命令定义的全局 IP 地址，如果 global_ip 为 0，就用 any 代替 0；如果 global_ip 是一台主机，就用 host 命令参数。

port 指的是服务所作用的端口，例如 www 使用 80，smtp 使用 25 等，我们可以通过服务名称或端口数字来指定端口。

protocol 指的是连接协议，比如 TCP、UDP 和 ICMP 等。

foreign_ip 表示可访问 global_ip 的外部 IP。对于任意主机，可以用 any 表示。如果 foreign_ip 是一台主机，就用 host 命令参数。

例 1

```
Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any
```

这个例子表示允许任何外部主机对全局地址为 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。Eq www 就是指允许或拒绝只对 www 的访问。

例 2

```
Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89
```

表示不允许外部主机 61.144.51.89 对任何全局地址进行 FTP 访问。

例 3

```
Pix525(config)#conduit permit icmp any any
```

表示允许 icmp 消息向内部和外部通过。

例 4

```
Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3
Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any
```

这个例子说明了 static 和 conduit 的关系。192.168.0.3 在内网是一台 Web 服务器，现在希望外网的用户能够通过 PIX 防火墙得到 Web 服务，所以先做 static 静态映射，即 192.168.0.3 ->61.144.51.62(全局)，然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 HTTP 访问。

3. 配置 fixup 协议

fixup 命令的作用是启用、禁止、改变一个服务或协议通过 PIX 防火墙，由 fixup 命令指定的端口是 PIX 防火墙要侦听的服务。

例 1

```
Pix525(config)#fixup protocol ftp 21
```

表示启用 FTP 协议，并指定 FTP 的端口号为 21。

例 2

```
Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 1080
```

表示为 HTTP 协议指定 80 和 1080 两个端口。

例 3

```
Pix525(config)#no fixup protocol smtp 80
```

表示禁用 SMTP 协议。

4. 设置 telnet

telnet 有一个版本的变化，在 PIX OS 5.0(PIX 操作系统的版本号)之前，只能从内部网络上的主机通过 telnet 访问 PIX。在 PIX OS 5.0 及后续版本中，可以在所有的接口上启用 telnet 到 PIX 的访问。当从外部接口 telnet 到 PIX 防火墙时，telnet 数据流需要用 IPSec 提供保护，也就是说用户必须配置 PIX 来建立一条到另外一台 PIX 路由器或 vpn 客户端的 IPSec 隧道。另外就是在 PIX 上配置 SSH，然后用 SSH Client 从外部 telnet 到 PIX 防火墙，PIX 支持 SSH1 和 SSH2，不过 SSH1 是免费软件，SSH2 是商业软件。相比之下，Cisco 路由器的 telnet 就做得不怎么样了。

telnet 配置语法为：

```
telnet local_ip
```

提示：local_ip 表示被授权通过 telnet 访问到 PIX 的 IP 地址。如果不设此项，PIX 的配置方式只能由 console 进行。

6.1.2 典型例题分析

例 1 阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。(2017 年上半年下午试题二)

【说明】

某公司的网络拓扑结构图如图 6-1 所示。

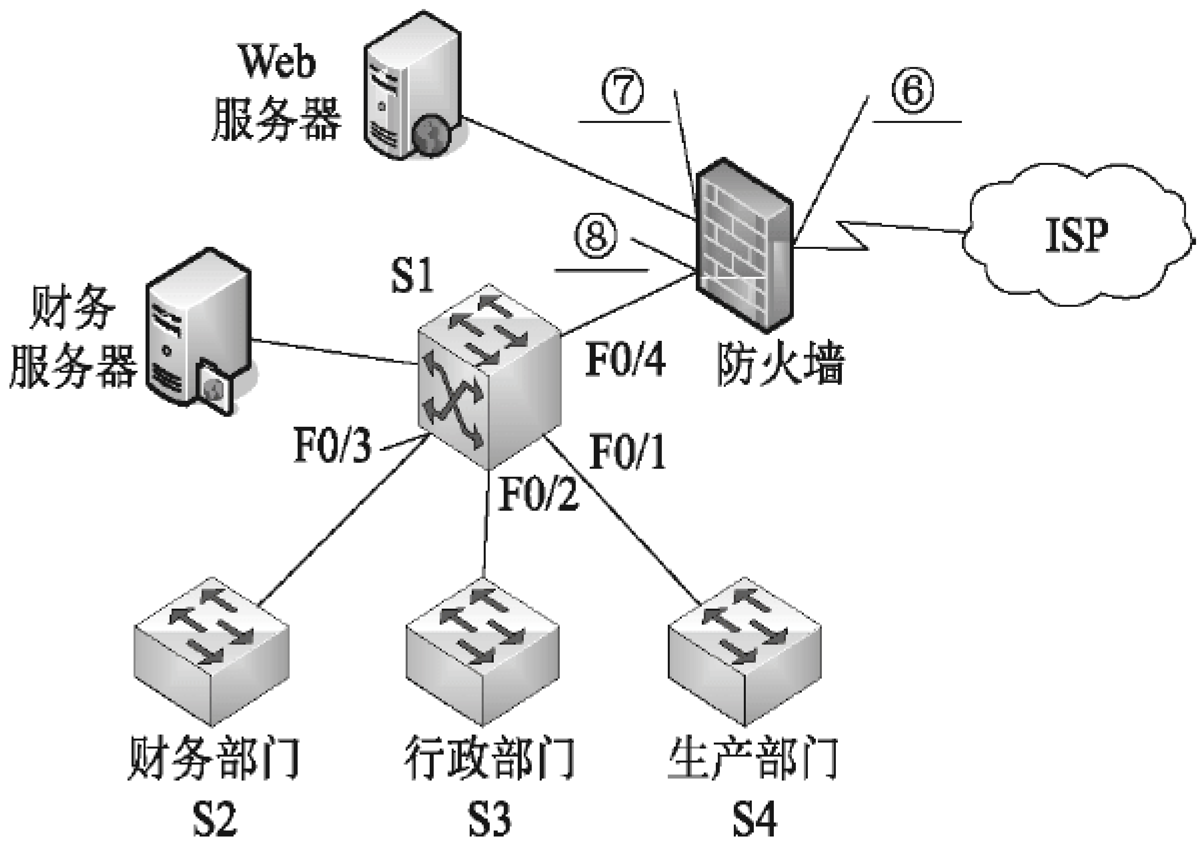


图 6-1　网络拓扑结构图

【问题 1】(共 5 分)

为了保障网络安全，该公司安装了一款防火墙，对内部网络、服务器以及外部网络进行逻辑隔离，其网络结构如图 6-1 所示。

包过滤防火墙使用 ACL 实现过滤功能，常用的 ACL 分为两种，编号为__(1)__的 ACL 根据 IP 报文的__(2)__域进行过滤，称为__(3)__；编号为__(4)__的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为__(5)__。

(1)～(5)备选项：

A. 标准访问控制列表	B. 扩展访问控制列表
C. 基于时间的访问控制列表	D. 1～99
E. 0～99	F. 100～199
G. 目的 IP 地址	H. 源 IP 地址
I. 源端口	J. 目的端口

【问题 2】(共 6 分)

如图 6-1 所示，防火墙的三个端口，端口⑥是__(6)__、端口⑦是__(7)__、端口⑧是__(8)__。

(6)～(8)备选项：

A. 外部网络　　B. 内部网络　　C. 非军事区

【问题 3】(共 9 分)

公司内部 IP 地址分配如表 6-1 所示。

表 6-1　公司内部 IP 地址分配

部门/服务器	IP 地址段
财务部门	192.168.9.0/24
生产部门	192.168.10.0/24
行政部门	192.168.11.0/24
财务服务器	192.168.100.1/24
Web 服务器	10.10.200.1/24

1. 为保护内网安全，防火墙的安全配置要求如下。

(1)　内外网用户均可访问 Web 服务器，特定主机 200.120.100.1 可以通过 Telnet 访问

Web 服务器。

(2) 禁止外网用户访问财务服务器，禁止财务部门访问 Internet，允许生产部门和行政部门访问 Internet。

根据以上需求，请按照防火墙的最小特权原则补充完成表 6-2。

表 6-2 配置信息表

序 号	源 地 址	源 端 口	目的地址	目的端口	协 议	规 则
1	Any	Any	(9)	(10)	WWW	允许
2	(11)	Any	10.10.200.1	(12)	Telnet	允许
3	(13)	Any	Any	Any	Any	(14)
4	Any	Any	Any	Any	Any	(15)

2. 若调换上面配置中的第 3 条和第 4 条规则的顺序，则__(16)__。

(16)备选项：

A. 安全规则不发生变化　　B. 财务服务器将受到安全威胁

C. Web 服务器将受到安全威胁　　D. 内网用户将无法访问 Internet

3. 在上面的配置中，是否实现了“禁止外网用户访问财务服务器”这条规则?

答案：

【问题 1】(1) D　(2) H　(3) A　(4) F　(5) B

【问题 2】(6) A　(7) C　(8) B

【问题 3】

1. (9) 10.10.200.1　(10) 80　(11) 200.120.100.1　(12) 23
   (13) 192.168.10.0　(14) 允许　(15) 拒绝

2. (16) D

3. 已经实现，除了允许的，其余均已经禁止。

解析：

【问题 1】访问控制列表用来限制使用者或设备，以达到控制网络流量、解决网络拥塞、提高安全性的目的。IP 访问控制列表主要有两种类型：标准访问控制列表和扩展访问控制列表。标准访问控制列表只对数据包中的源地址进行检查，以此来判定是否允许数据包通过，其表号为 1～99。扩展访问控制列表除了检查源地址和目的地址外，还可以检查指定的协议或端口号，来对数据包进行过滤，其表号为 100～199。

【问题 2】防火墙通常具有至少 3 个接口，使用防火墙时，至少产生了 3 个网络，描述如下。

内部区域(内网)。内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。

外部区域(外网)。外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。

非军事区(DMZ，又称停火区)。它是一个隔离的网络，或几个网络。位于区域内的主机

或服务器被称为堡垒主机。一般在非军事区内可以放置 Web、Mail 服务器等。停火区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许它们访问企业内部网络。

【问题 3】访问控制列表就是用来在路由技术的网络中，决定这些数据流量是应该被转发还是被丢弃的技术。因此访问控制列表就成了实现防火墙的重要手段。设置 ACL 的规则主要是：按顺序依行进行比较，从第一行起直到找到一个符合条件的行，符合之后，其余的行就无须比较了。默认在 ACL 中最后一行都隐藏拒绝所有，如果之前没找到一条 permit 语句，则意味着该包将被丢弃。所以每个 ACL 中都应该至少有一行 permit 语句，除非用户想把所有的数据包丢弃。

如果 3 和 4 两行的顺序调换，会导致内网的用户无法访问互联网。

禁止外网访问财务服务器已经实现，因为配置中除了被允许的，其余均已禁止。

例 2　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】 某公司通过 PIX 防火墙接入 Internet，网络拓扑如图 6-2 所示。

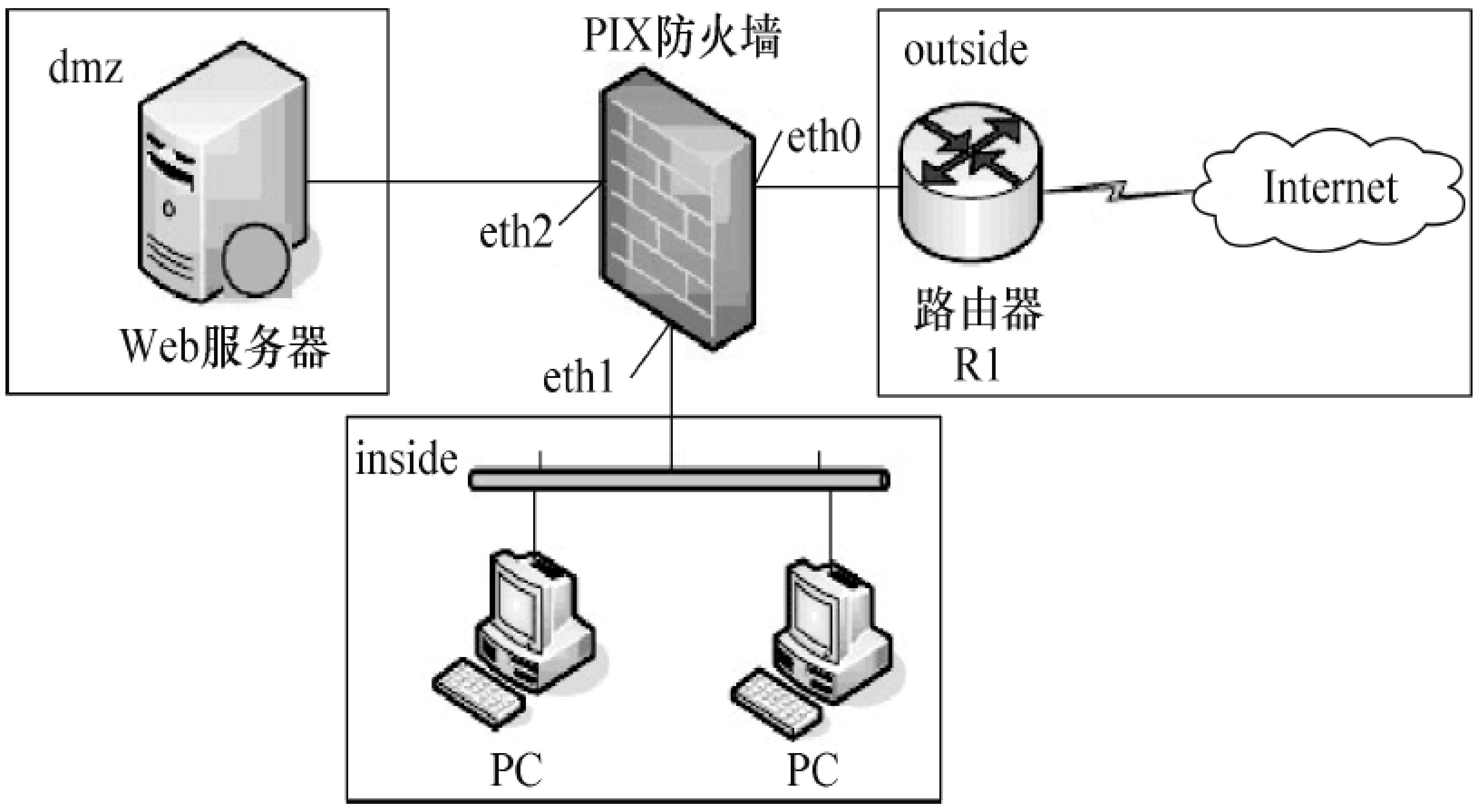


图 6-2　网络拓扑结构图

在防火墙上利用 show 命令查询当前配置信息如下。

```
PIX# show config
…
nameif eth0 outside security 0
nameif eth1 inside security 100
nameif eth2 dmz security 40
…
fixup protocol ftp 21          (1)
fixup protocol http 80
…
ip address outside 61.144.51.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
ip address dmz 10.10.0.1 255.255.255.0
…
global(outside) 1 61.144.51.46
nat(inside) 1 0.0.0.0 0.0.0.0
…
```

```
route outside 0.0.0.0 0.0.0.0 61.144.51.45 1   (2)
…
```

【问题 1】(4 分)

解析(1)、(2)处画线语句的含义。

【问题 2】(6 分)

根据配置信息，填充表 6-3。

表 6-3 配置信息表

域 名 称	接口名称	IP 地址	IP 地址掩码
inside	eth1	(3)	255.255.255.0
ouside	eth0	61.144.51.42	(4)
dmz	(5)	(6)	255.255.255.0

【问题 3】(2 分)

根据所显示的配置信息，由 inside 域发往 Internet 的 IP 分组，在到达路由器 R1 时的源 IP 地址是 (7) 。

【问题 4】(3 分)

如果需要在 DMZ 域的服务器(IP 地址为 10.10.0.100)上对 Internet 用户提供 Web 服务(对外公开 IP 地址为 61.144.51.43)，请补充完成下列配置命令。

```
PIX(config)# static(dmz, outside)  (8)   (9)
PIX(config)# conduit permit tcp host  (10)  eq www any
```

答案：

【问题 1】

(1)添加可监听的 FTP 服务端口 21

(2)定义外部默认路由 61.144.51.45，跳数为 1

【问题 2】

(3)192.168.0.1　(4)255.255.255.248　(5)eth2　(6)10.10.0.1

【问题 3】

(7)61.144.51.46

【问题 4】

(8)10.10.0.100　(9)61.144.51.43　(10)61.144.51.43

解析：

本题考查防火墙的配置。

【问题 1】 fixup 命令的作用是启用、禁止和改变一个服务或协议。通过 PIX 防火墙配置，PIX 防火墙侦听由 fixup 命令指定的端口。

```
fixup protocol ftp 21
#启用 ftp 协议，并指定 ftp 的端口号为 21
```

route 命令用于设置指向内网和外网的静态路由。

```
route outside 0.0.0.0 0.0.0.0 61.144.51.45 1
```

```
#定义外部默认路由 61.144.51.45，跳数为 1
```

【问题 2】 程序解释如下。

```
…
nameif eth0 outside security 0   eth0
#被命名为外部接口(outside)，安全级别是 0
nameif eth1 inside security 100   eth1
#被命名为内部接口(inside)，安全级别是 100
nameif eth2 dmz security 40 dmz
#被命名为非军事区接口(outside)，安全级别是 40
…

ip address outside 61.144.51.42 255.255.255.248
#设置外部接口的 IP 为 61.144.51.42，子网掩码为 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
#设置内部接口的 IP 为 192.168.0.1，子网掩码为 255.255.255.0
ip address dmz 10.10.0.1 255.255.255.0
#设置 DMZ 接口的 IP 为 10.10.0.1，子网掩码为 255.255.255.0
```

【问题 3】 global(outside) 1 61.144.51.46 表示内网的主机通过 PIX 防火墙访问外网时，PIX 防火墙将使用 61.144.51.46 为要访问外网的主机分配一个全局 IP 地址。

nat(inside) 1 0.0.0.0 0.0.0.0 表示启用 nat，内网的所有主机都可以访问外网。

【问题 4】

```
PIX(config)# static(dmz, outside) 10.10.0.100 61.144.51.43
#任何外部主机访问 61.144.51.43 时，防火墙都映射到 10.10.0.100 这个地址
PIX(config)# conduit permit tcp host 61.144.51.43 eq www any
#允许任何外部主机对全局地址 61.144.51.43 的这台主机进行 http 访问
```

6.1.3　同步练习

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。(2016 年下半年下午试题一)

【说明】

某企业的行政部、技术部和生产部分布在三个区域，随着企业对信息化需求的提高，现拟将网络出口链路由单链路升级为双链路，提升 ERP 系统服务能力以及加强员工上网行为管控。网络管理员依据企业现有网络和新的网络需求设计了该企业网络拓扑图 6-3，并对网络地址重新进行了规划，其中防火墙设备继承了传统防火墙与路由功能。

【问题 1】 (4 分)

在图 6-3 的防火墙设备中，配置双出口链路有提高总带宽、__(1)__、链路负载均衡作用。通过配置链路聚合来提高总带宽，通过配置__(2)__来实现链路负载均衡。

【问题 2】 (4 分)

防火墙工作模式有路由模式、透明模式、混合模式，若该防火墙接口均配有 IP 地址，则防火墙工作在__(3)__模式。该模式下，ERP 服务器部署在防火墙的__(4)__区域。

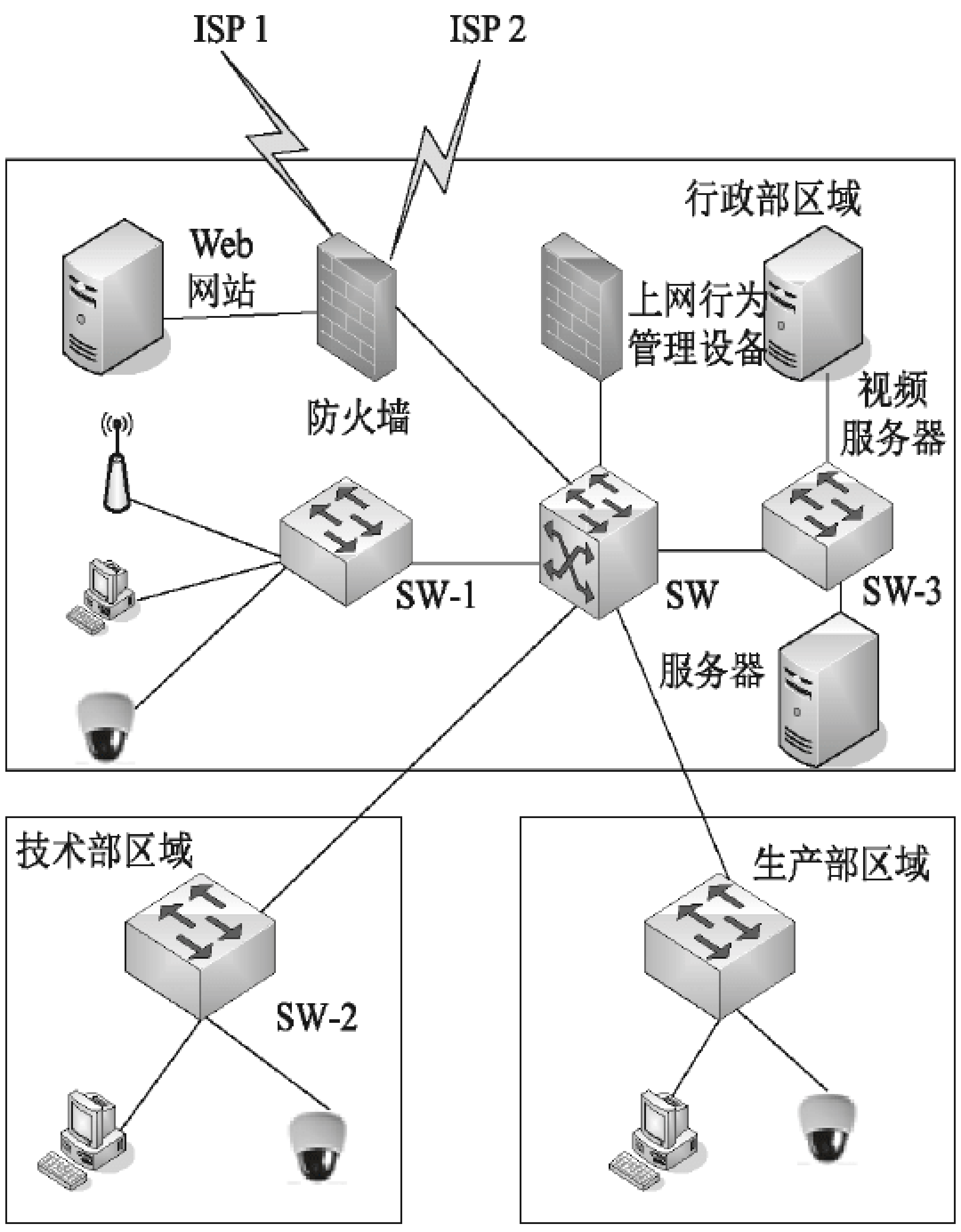


图 6-3　网络拓扑图

【问题 3】 (4 分)

若地址规划如表 6-4 所示，从 IP 规划方案看该地址的配置可能有哪些方面的考虑?

表 6-4　地址规划表

位置或系统	VLAN ID	地址区间	信息点数量	备　注
行政部	10～13	192.168.10.0～192.168.13.0	60	网段按楼层分配，每个网段末位地址为网关
技术部	16～17	192.168.14.0～192.168.17.0	80	
生产部	18～20	192.168.18.0～192.168.20.0	30	
无线网络	22	192.168.22.0		行政楼区域部署
监控网络	23	192.168.23.0	30	信息点分散
ERP	30	192.168.30.0		

【问题 4】 (3 分)

该网络拓扑中，上网行为管理设备的位置是否合适？请说明理由。

【问题 5】 (3 分)

该网络中有无线节点的接入，在安全管理方面应采取哪些措施?

【问题 6】(2 分)

该网络中视频监控系统与数据业务共用网络带宽，存在哪些弊端?

6.1.4　同步练习参考答案

答案:

【问题 1】(1)链路备份/冗余　(2)策略路由

【问题 2】(3)路由　(4)内部/inside

【问题 3】各部门终端数的扩展考虑，增加部门或部门 VLAN 的考虑，监控以及部门中信息点增加的扩展考虑。

【问题 4】不合适，应该部署在防火墙与核心交换机间，使用跨接/串联的方式接入。因为需要对用户上网行为进行管控，需要保证上网数据流经上网行为管理设备。

【问题 5】接入认证、无线加密、隐藏 SSID、授权管理、审计管理(本题分值为 3 分，答对 3 个即可)

【问题 6】视频监控系统业务流量大，如果带宽不足会影响数据业务的通信速率。

解析：

【问题 1】

本题考查企业网络的规划相关知识，包括网络接入策略、网络拓扑规划、服务器以及网络安全设备部署等的综合应用。

此类题目要求考生具备较为丰富的网络构建经验，具有对题目给出的网络环境进行分析的能力，对于题目给出的某企业网络的应用，进行分析并说明该网络部署的依据。

在本题中，防火墙部署在企业网的出口，起到了安全隔离内部网与外部网的作用，当两条 ISP 链路接入防火墙时，可以起到提高总带宽、链路冗余和负载均衡的作用。一般而言，增加出口链路数量必然会增加企业网的出口总带宽，降低网络拥塞，避免网络瓶颈的出现。两条链路也可以起到链路冗余的作用，当一条链路不可用或者异常中断时，故障链路上的数据可以自动地切换到正常链路之上，可以避免业务的中断。通过策略路由对网络请求进行重定向和内容管理，实现数据在两条链路上的负载均衡。

【问题 2】

防火墙三种工作模式的区别如下。

① 路由模式：内部网络和外部网络属于不同的子网，需要重新规划原有的网络拓扑，接口需要配置 IP 地址，接口所在的安全区域是三层区域。

② 透明模式：内部网络和外部网络属于相同的子网，无须改变原有的网络拓扑，接口不能配置 IP 地址，接口所在的安全区域是二层区域。

③ 混合模式：混合模式介于路由模式和透明模式，既可以配置接口工作在路由模式(接口具有 IP 地址)，又可以配置接口工作在透明模式(接口无 IP 地址)，主要在 Eudemon 1000G 进行双机热备时使用。

由于防火墙接口均配有 IP 地址，很明显工作于路由模式；在拓扑图上可以直接观察到 Web 服务器部署在 DMZ(非军事)区域，ERP 服务器部署在内网区域。

【问题 3】

从 IP 规划方案来看，每个部门划分三个 VLAN，分配的 IP 子网为 192.168.10.0～192.168.20.0，其他未被使用的 192.168.X.0 子网可供扩展的 VLAN 或部门使用，每个 VLAN 规划的子网可用主机数大于目前的信息点数，从以后的网络扩展角度来看，VLAN 中或部门的信息点数的增加，包括无线网络和监控网络的信息点的增加，都可以直接使用未使用的可用主机地址，而不需要重新增加子网或 VLAN。

【问题 4】

上网行为管理设备的位置应该保证内网用户的上网流量经过其设备，从而实现行为管理策略。

【问题 5】

WLAN 基本安全主要是无线接入和加密,其措施可以有 SSID 隐藏、WEP 或 WPA/WAP2 加密、MAC 地址过滤等。当然对于更负责的安全管理还可以结合 AAA 系统做认证、授权、计费管理甚至审计等。

【问题 6】

该网络中的视频监控系统与数据业务共享带宽，主要的弊端有两个方面，一是视频监控数据量较大并且始终占用一定量的带宽资源，会影响业务数据；二是视频监控系统未做安全防范部署说明，在内部网络中存在数据泄露风险。

6.2 VPN 配置

6.2.1 考点辅导

6.2.1.1 VPN 介绍

VPN(虚拟专用网络)可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障，其拓扑结构如图 6-4 所示。

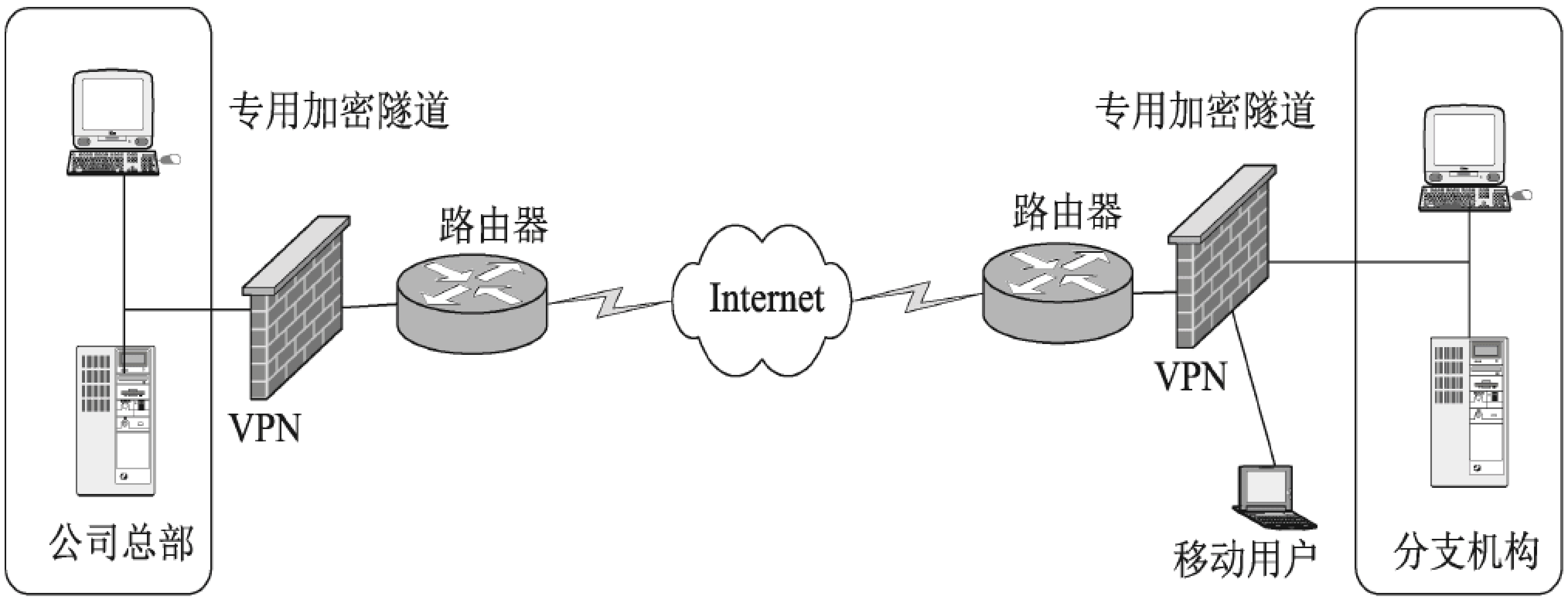


图 6-4 VPN 实现网络拓扑结构图

VPN 技术是将 Internet 作为计算机网络主干的一种网络模式，其基本特点就是化公为私，使每个企业可以临时从公用网中挖走一部分地盘供自己专用。所以企业网络想连接到哪里都可以，保密性、安全性和可管理性的问题也容易解决，而且还可以降低网络的使用成本。据估计，VPN 可以使企业的远程访问和分支机构连接成本降低 50%以上。

打个比方说，如果一个外企员工在驻北京办事处工作，其公司总部却在新加坡，只能通过电话拨号到新加坡的亚太总部来收发电子邮件和访问公司的内部 Web，电话费用非常高，而且通信速度也不理想。但是，假如新加坡亚太总部已经和 Internet 联网，那么只要驻

北京办事处申请一个本地的 Internet 账号，然后借助 Internet 这张大网，就可以与亚太总部联上了。这样不仅可以在短时间内与公司联网，而且只需付出低廉的本地电话费和 Internet 使用费。虚拟专用网还可以提供通信安全和联网速度保障。VPN 的效果相当于在 Internet 中自动拉一条虚拟专线，这条专线叫隧道(Tunnel)。

6.2.1.2　VPN 的基本用途

1. 通过 Internet 实现远程用户访问

虚拟专用网络支持以安全的方式通过公共互联网络远程访问企业资源。与使用专线拨打长途电话连接企业的网络接入服务器(NAS)不同，虚拟专用网络用户首先拨通本地 ISP 的 NAS，然后 VPN 软件利用与本地 ISP 建立的连接在拨号用户和企业 VPN 服务器之间创建一个跨越 Internet 或其他公共互联网络的虚拟专用网络。

2. 通过 Internet 实现网络互联

可以采用以下两种方式使用 VPN 连接远程局域网络。

1)　使用专线连接分支机构和企业局域网

不需要使用价格昂贵的长距离专用电路，分支机构和企业端路由器可以使用各自本地的专用线路通过本地的 ISP 连通 Internet。VPN 软件使用与本地 ISP 建立的连接和 Internet 网络，在分支机构和企业端路由器之间创建一个虚拟专用网络。

2)　使用拨号线路连接分支机构和企业局域网

不同于传统的使用连接分支机构路由器的专线拨打长途电话连接企业 NAS 的方式，分支机构端的路由器可以通过拨号方式连接本地 ISP。VPN 软件使用与本地 ISP 建立起的连接，在分支机构和企业端路由器之间创建一个跨越 Internet 的虚拟专用网络。

注意：以上两种方式通过使用本地设备，在分支机构和企业部门与 Internet 之间建立连接。无论是在客户端还是服务器端都是通过拨打本地接入电话建立连接，因此 VPN 可以大大节省连接的费用。建议作为 VPN 服务器的企业端路由器使用专线连接本地 ISP。VPN 服务器必须一天 24 小时对 VPN 数据流进行监听。

3. 连接企业内部网络计算机

在企业的内部网络中，考虑到一些部门可能存储有重要数据，为确保数据的安全性，传统的方式只能把这些部门同整个企业网络断开形成孤立的小网络。这样做虽然保护了部门的重要信息，但是由于物理上的中断，使其他部门的用户无法访问该网络，造成通信上的困难。

而采用 VPN 方案，通过使用一台 VPN 服务器既能够实现与整个企业网络的连接，又可以保证保密数据的安全性。路由器虽然也能够实现网络之间的互联，但是并不能对流向敏感网络的数据进行限制。企业网络管理人员通过使用 VPN 服务器，指定只有符合特定身份要求的用户才能连接 VPN 服务器获得访问敏感信息的权利。此外，它还可以对所有 VPN 数据进行加密，从而确保数据的安全性。没有访问权限的用户无法看到部门的局域网络。

6.2.1.3　VPN 的基本要求

一般来说，企业在选用一种远程网络互联方案时，都希望能够对访问企业资源和信息

的要求加以控制，因此所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接，实现不同分支机构之间的资源共享，又能够确保企业数据在公共互联网络或企业内部网络上传输时安全性不受破坏。所以，最低限度上一个成功的 VPN 方案应当能够满足以下所有方面的要求。

1. 用户验证

VPN 方案必须能够验证用户身份并严格控制只有授权用户才能访问 VPN。另外，方案还必须能够提供审计和计费功能，显示何人在何时访问了何种信息。

2. 地址管理

VPN 方案必须能够为用户分配专用网络上的地址并确保地址的安全性。

3. 数据加密

VPN 方案必须对通过公共互联网络传递的数据进行加密，确保网络其他未授权的用户无法读取该信息。

4. 密钥管理

VPN 方案必须能够生成并更新客户端和服务器的加密密钥。

5. 多协议支持

VPN 方案必须支持公共互联网络上普遍使用的基本协议，包括 IP 和 IPX 协议等。以点对点隧道协议(PPTP)或第二层隧道协议(L2TP)为基础的 VPN 方案既能够满足以上所有的基本要求，又能够充分利用遍及世界各地的 Internet 互联网络的优势。其他方案，包括安全 IP 协议(IPSec)，虽然不能满足上述全部要求，但是仍然适用于特定的环境中。本文以下部分将主要讨论有关 VPN 的概念、协议和部件。

6.2.1.4　VPN 的实现

VPN 的建立可以基于几种不同的网络协议，其中最常见的是利用 PPTP 协议的 VPN 工作方式。

基于 PPTP 协议(点对点隧道协议)网络连接方式的 VPN，允许一台客户机通过一个公共网络(如 Internet)建立一个秘密的多协议 VLAN 网络。因此，它可以使公司远端的员工通过 Internet 而不是直接拨号连接公司的网络。这就是说，通过 PPTP 的封装，可以使非 IP 网络获得 Internet 通信的优点。PPTP 是微软和其他厂家支持的标准，它是 PPP 协议的扩展，可以通过 Internet 建立多协议 VPN。

VPN 模仿点对点连接技术，依靠 Internet 服务提供商(ISP)和其他的网络服务提供商(NSP)在公用网中建立自己专用的“隧道”，让数据包通过这条隧道传输。对于不同的信息来源，可分别给它们开出不同的隧道。于是，兼容性问题、不同的服务质量要求以及其他的麻烦都迎刃而解了。

PPTP 协议是一种第二层隧道协议。为了传输来自不同网络的数据包，最普遍使用的方法是先把各种网络协议(IP、IPX 和 AppleTalk 等)封装到 PPP 中，再把这整个数据包装入隧道协议里。这种双层封装形成的数据包需靠第二层协议进行传输，所以称之为“第二层隧道”。另一种方法是把各种网络协议直接装入隧道协议中，由于形成的数据包需靠第三层

协议进行传输，所以称之为“第三层隧道”。

除了基于 PPTP 模式的 VPN 之外，VPN 还可以基于以下几种协议。

1. GRE——通用路由封装

GRE 协议是由 Cisco 和 Net-smiths 等公司于 1994 年提交给 IETF 的，相关文档为 RFC1701 和 RFC1702。目前有多数厂商的网络设备均支持 GRE 隧道协议。

GRE 规定了如何用一种网络协议去封装另一种网络协议的方法。GRE 隧道由两端的源 IP 地址和目的 IP 地址来定义，允许用户使用 IP 包封装 IP、IPX 和 AppleTalk 包，并支持全部路由协议(如 RIP2 和 OSPF 等)。通过 GRE，用户可以利用公共 IP 网络连接 IPX 网络和 AppleTalk 网络，还可以使用保留地址进行网络互联，或者对公网隐藏企业网的 IP 地址。GRE 只提供了数据包的封装，没有加密功能来防止网络侦听和攻击，所以在实际环境中经常与 IPSec 一起使用，由 IPSec 提供用户数据的加密，从而给用户提供更好的安全性。

2. L2TP——第二层隧道协议

除 Microsoft 外，还有一些厂家也做了许多开发工作。PPTP 能支持 Macintosh 和 UNIX，而 Cisco 的 L2F(Layer2 Forwarding)也是一个隧道协议。Microsoft、Cisco 和其他一些网络厂商正一起努力使 L2F 与 PPTP 融合，产生一个新的 L2TP 协议。L2TP 和 PPTP 十分相似，因为 L2TP 有一部分就是采用 PPTP 协议，这两个协议都允许客户通过其间的网络建立隧道。L2TP 还支持信道认证，但它没有规定信道保护的方法。

3. IPSec——IP Security

开发这个协议的目的是解决当前协议中存在的一些缺点。IPSec 是由 IETF IP 安全性工作组定义的协议集，用于确保网络层之间的安全通信。该协议草案建议使用 IPSec 协议集保护 IP 网和非 IP 网上的 L2TP 业务，并规定了如何共同使用 IPSec 和 L2FP。下一小节将对 IPSec 的配置作详细介绍。

6.2.1.5　硬件平台的 VPN 配置

VPN 的配置是当代技术领域的热点问题，也是下午考试的重点内容，尤其在最近几年几乎每年必考。为了帮助考生快速掌握 VPN 的具体实现，下面以 Cisco 路由器为例，简单介绍一下 VPN 的配置过程以及相关命令。

1. 场景描述

一边服务器的网络子网为 192.168.1.0/24，路由器为 100.10.15.1；另一边服务器的网络子网为 192.168.10.0/24，路由器为 200.20.25.1。

2. 执行步骤

(1) 确定一个预先共享的密钥(保密密码)(以下例子保密密码假设为 noIP4u)。
(2) 为 SA 协商过程配置 IKE。
(3) 配置 IPSec。

3. 配置 IKE

```
Shelby(config)#crypto isakmp policy 1
```

说明：policy 1 表示策略 1，假如想多配几个 VPN，可以写成 policy 2、policy3……

```
Shelby(config-isakmp)#group 1
```

说明：除非购买高端路由器，或是 VPN 通信比较少，否则最好使用 group 1 长度的密钥。group 命令有两个参数值，即 1 和 2。参数值 1 表示使用 768 位密钥，参数值 2 表示使用 1024 位密钥。显然后一种密钥安全性高，但消耗更多的 CPU 和时间。

```
Shelby(config-isakmp)#authentication pre-share
```

说明：告诉路由器要使用预先共享的密码。

```
Shelby(config-isakmp)#lifetime 3600
```

说明：对生成新 SA 的周期进行调整。这个值以秒为单位，默认值为 86 400，也就是一天。值得注意的是，两端的路由器都要设置相同的 SA 周期，否则 VPN 在正常初始化之后，将会在较短的一个 SA 周期到达中断。

```
Shelby(config)#crypto isakmp key noIP4u address 200.20.25.1
```

说明：返回到全局设置模式确定要使用的预先共享密钥和指定 VPN 另一端路由器 IP 地址，即目的路由器 IP 地址。相应的在另一端路由器的配置也和以上命令类似，只不过把 IP 地址改成 100.10.15.1。

4. 配置 IPSec

```
Shelby(config)#access-list 130 permit ip 192.168.1.0 0.0.0.255 172.16.10.0
0.0.0.255
```

说明：在这里使用的访问列表号不能与任何过滤访问列表相同，应该使用不同的访问列表号来标识 VPN 规则。

```
Shelby(config)#crypto ipsec transform-set vpn1 ah-md5-hmac esp-des
esp-md5-hmac
```

说明：在这里两端路由器唯一不同的参数是 vpn1，这是为这种选项组合所定义的名称。在两端的路由器上，这个名称可以相同，也可以不同。以上命令是定义所使用的 IPSec 参数。为了加强安全性，要启动验证报头。由于两个网络都使用私有地址空间，需要通过隧道传输数据，因此还要使用安全封装协议。最后，还要定义 DES 作为保密密钥的加密算法。

```
Shelby(config)#crypto map shortsec 60 ipsec-isakmp
```

说明：以上命令为定义生成新保密密钥的周期。如果攻击者破解了保密密钥，他就能够解开使用同一个密钥的所有通信。基于这个原因，我们要设置一个较短的密钥更新周期。比如，每分钟生成一个新密钥。这个命令在 VPN 两端的路由器上必须匹配。参数 shortsec 是我们给这个配置定义的名称，稍后可以将它与路由器的外部接口建立关联。

```
Shelby(config-crypto-map)#set peer 200.20.25.1
```

说明：这是标识对方路由器的合法 IP 地址。在远程路由器上也要输入类似命令，只是对方路由器地址应该是 100.10.15.1。

```
Shelby(config-crypto-map)#set transform-set vpn1
Shelby(config-crypto-map)#match address 130
```

说明：这两个命令分别用于标识这个连接的传输设置和访问列表。

```
Shelby(config)#interface s0
Shelby(config-if)#crypto map shortsec
```

说明：将刚才定义的密码图应用到路由器的外部接口上。

6.2.1.6　Windows 平台的 VPN 配置

1. 创建 VPN 服务器

Windows Server 2003 中 VPN 服务被称为“路由和远程访问”，默认状态已经安装。只需对此服务进行必要的配置使其生效即可。创建 VPN 服务器的步骤如下。

(1)　以管理员身份登录 Windows Server 2003，依次选择“开始”→“管理工具”命令，运行“配置您的服务器向导”命令，启动如图 6-5 所示的“配置您的服务器向导”对话框。

(2)　单击“下一步”按钮，在如图 6-6 所示的“预备步骤”界面中，单击“下一步”按钮。

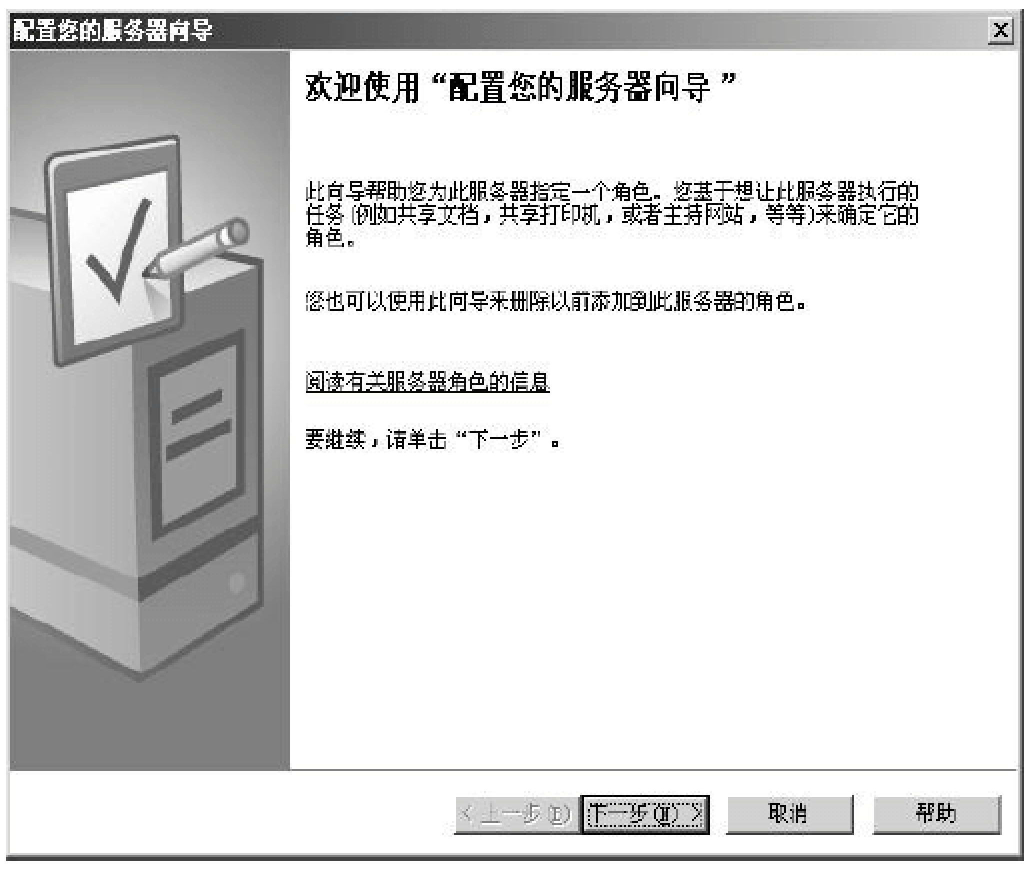


图 6-5　“配置您的服务器向导”对话框

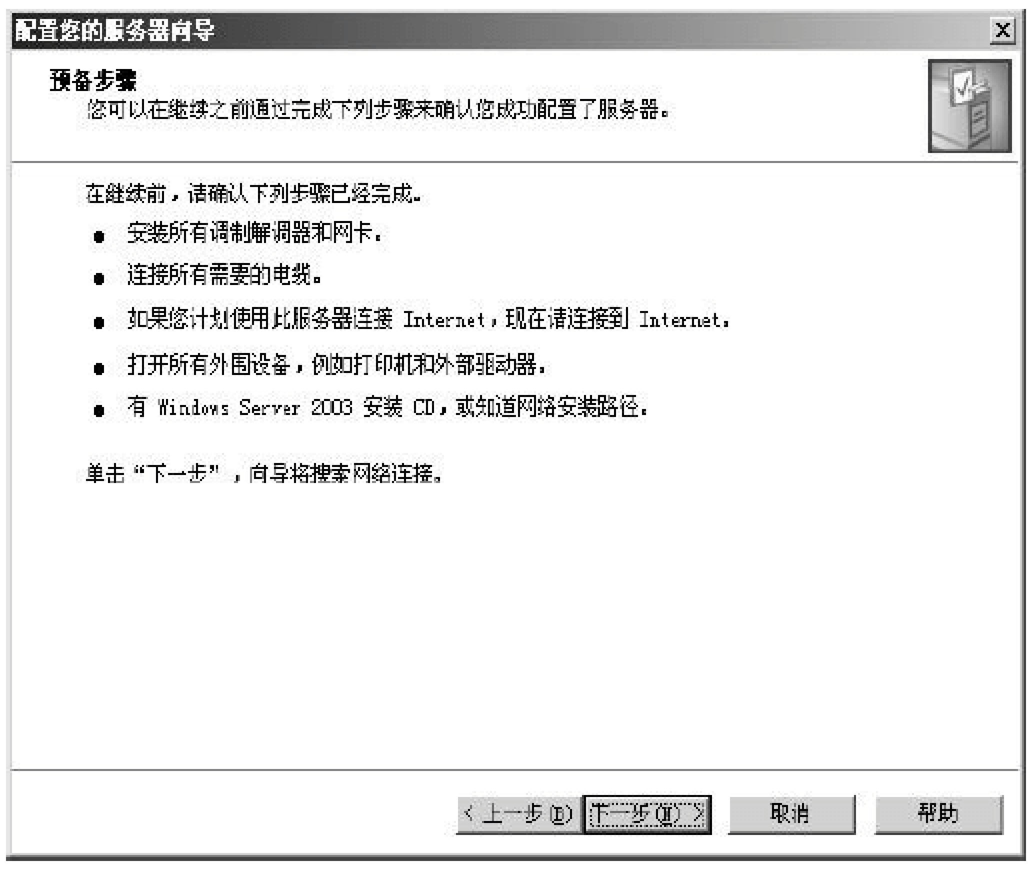


图 6-6　“预备步骤”界面

(3)　在如图 6-7 所示的“服务器角色”界面中，选择“远程访问/VPN 服务器”选项，单击“下一步”按钮。

(4)　在如图 6-8 所示的“选择总结”界面中，单击“下一步”按钮。

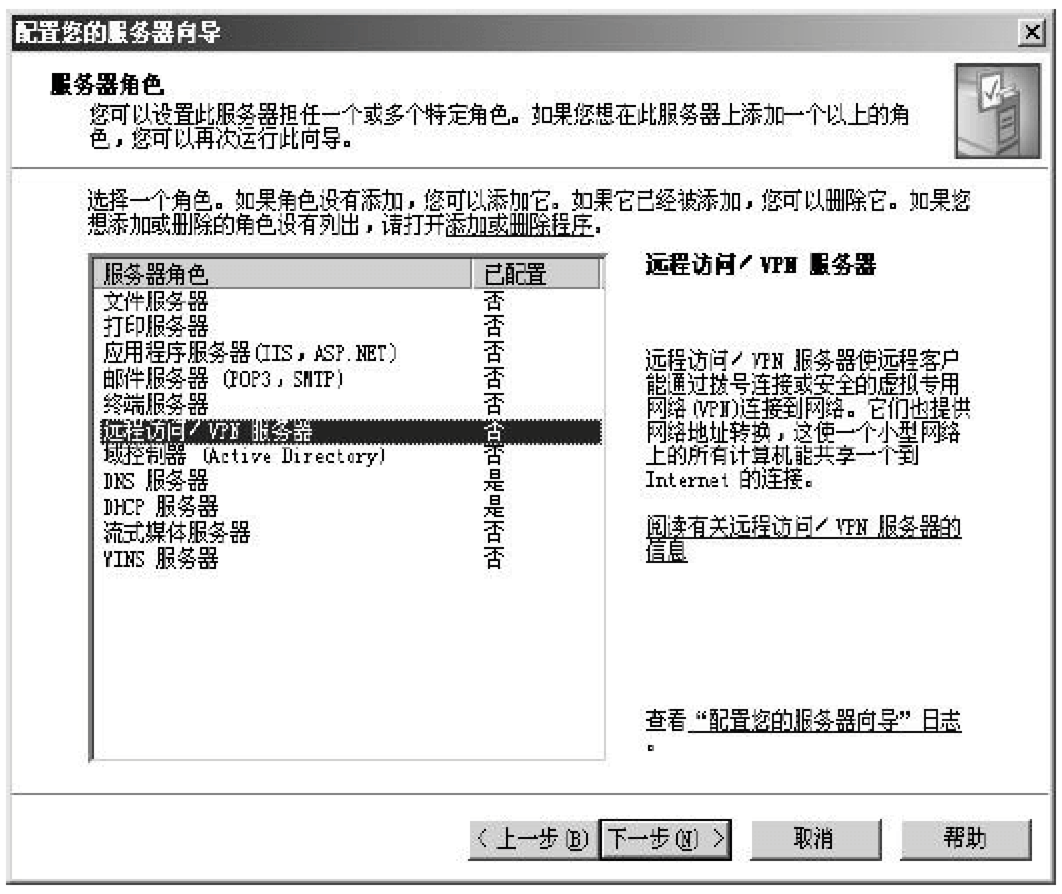


图 6-7　“服务器角色”界面

图 6-8　“选择总结”界面

(5) 系统启动“欢迎使用路由和远程访问服务器安装向导”界面，如图 6-9 所示，单击“下一步”按钮。

(6) 在如图 6-10 所示的“配置”界面中，选中“远程访问(拨号或 VPN)”单选按钮，然后单击“下一步”按钮。

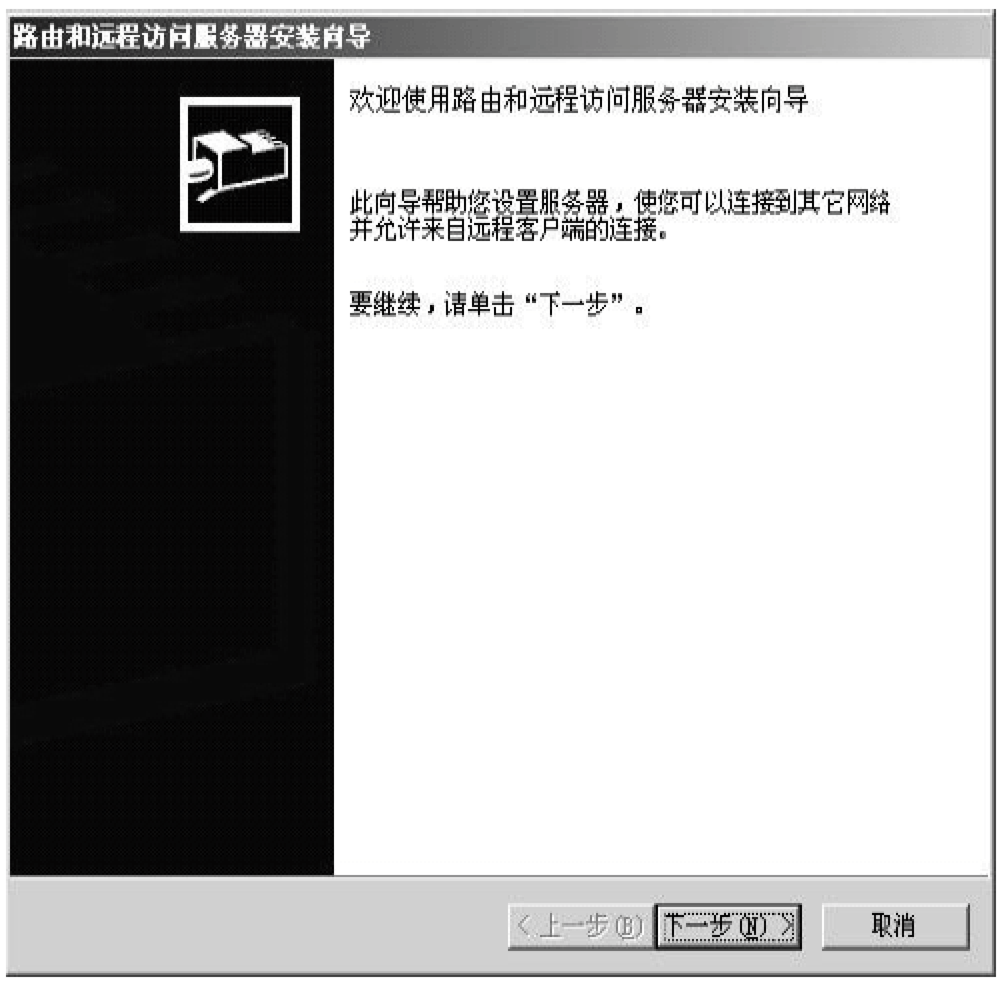


图 6-9 “欢迎使用路由和远程访问服务器安装向导”界面

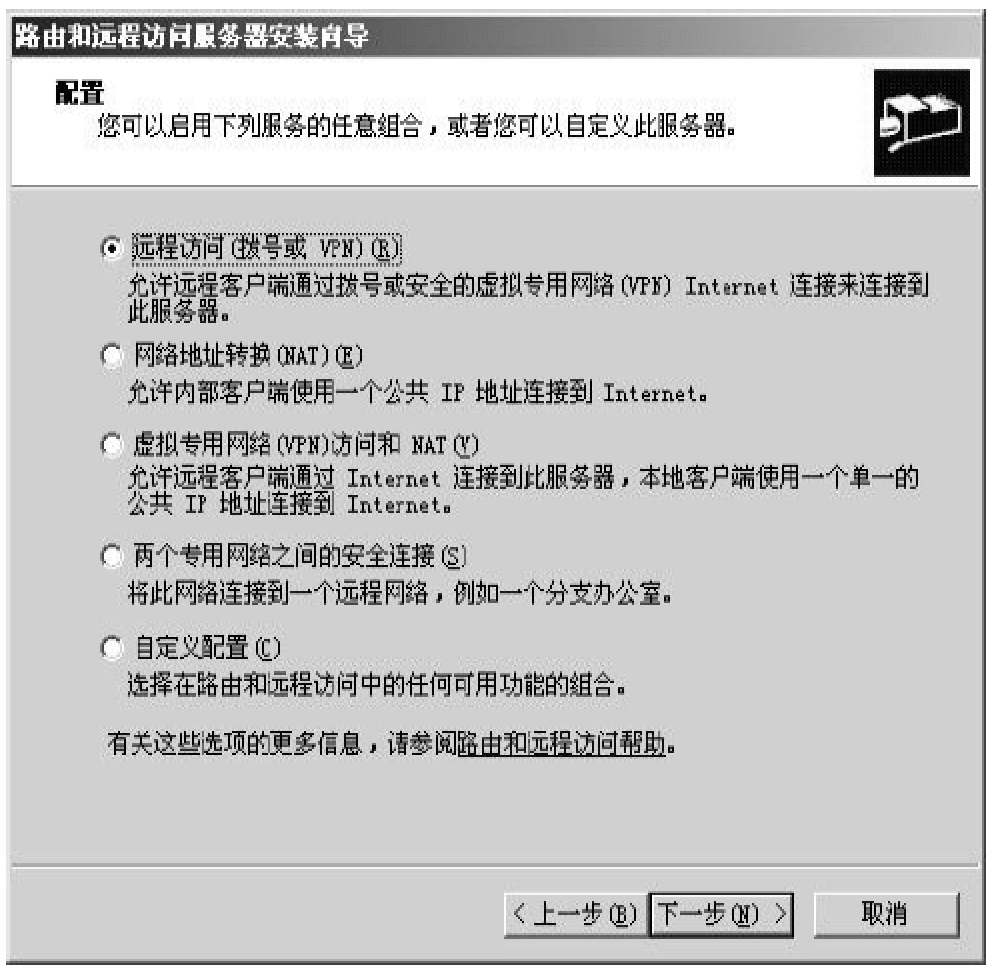


图 6-10 “配置”界面

(7) 在如图 6-11 所示的“远程访问”界面中，选中 VPN 复选框，单击“下一步”按钮。

(8) 接下来，向导界面将列出系统上所有的网络接口。选择与 Internet 相连的网络接口，如图 6-12 所示，单击“下一步”按钮。

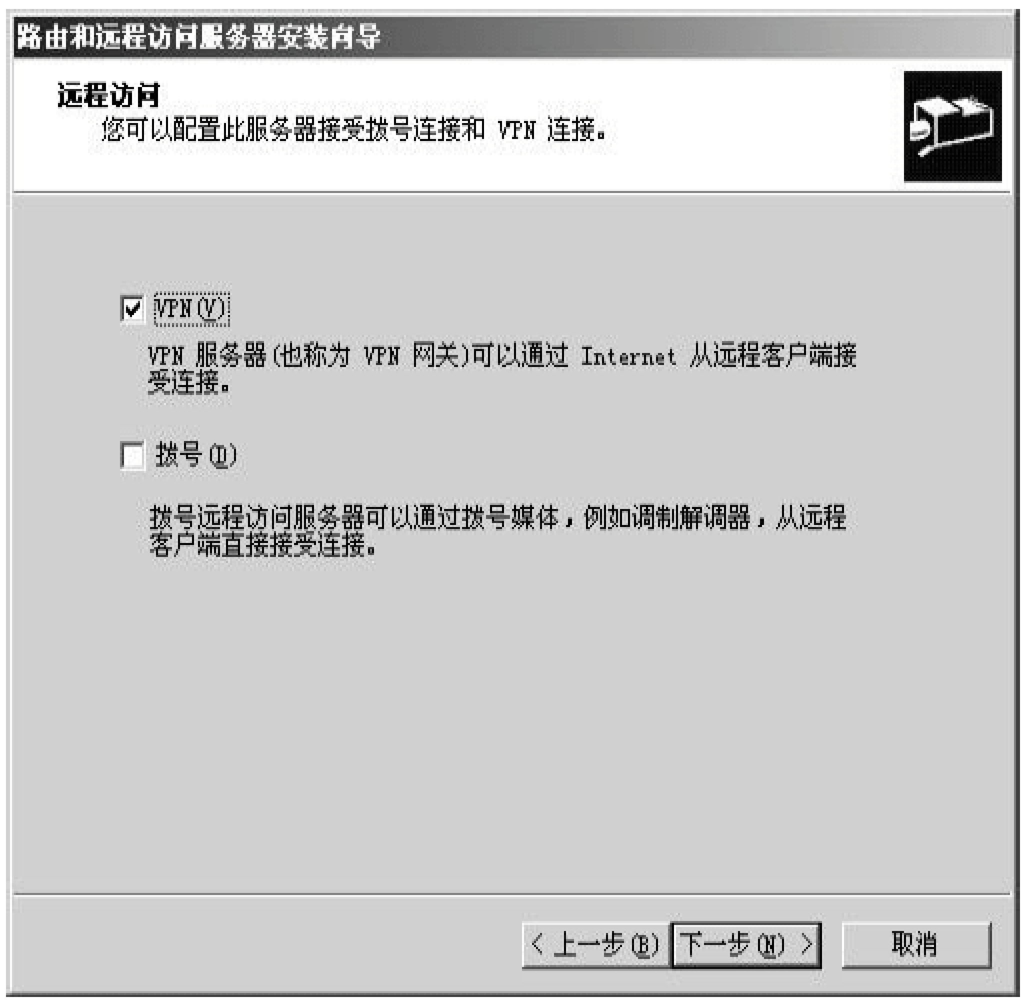


图 6-11 “远程访问”界面

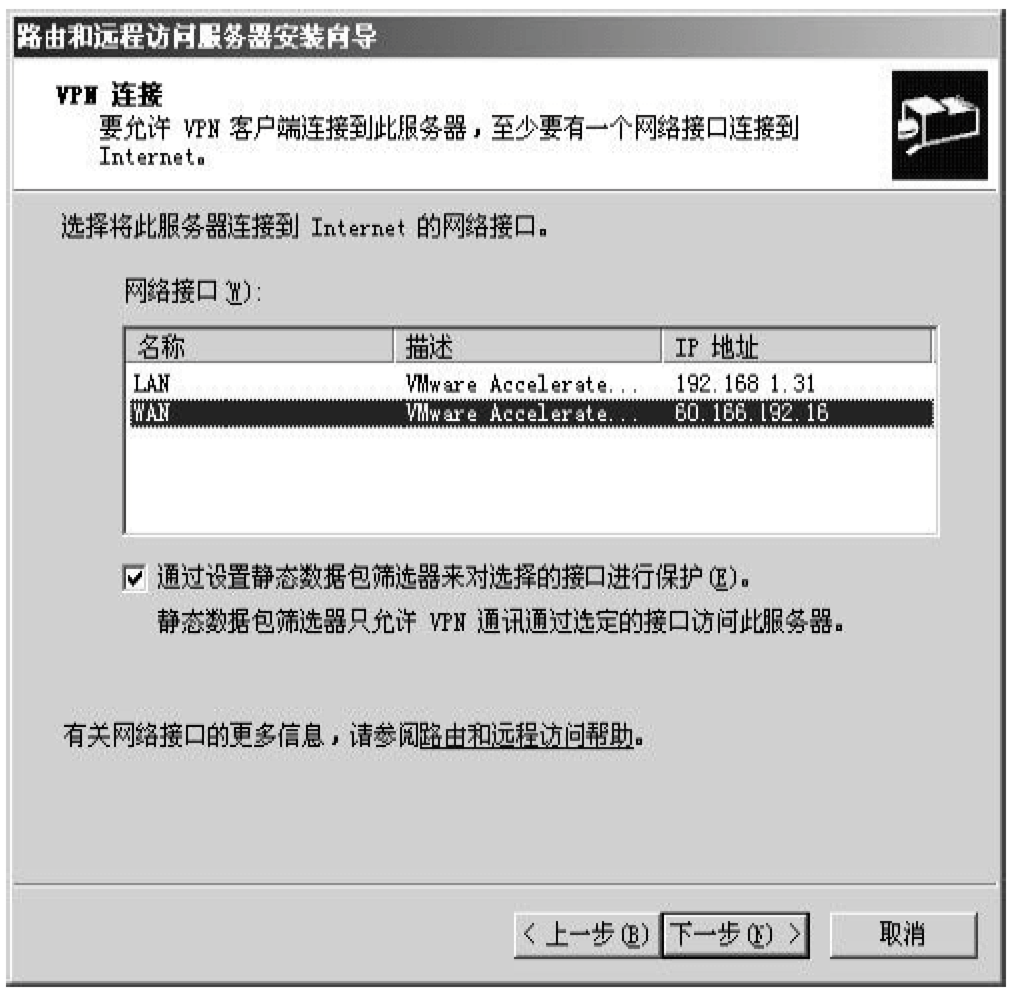


图 6-12 选择网络接口

(9) 在如图 6-13 所示的“IP 地址指定”界面中，需要选择如何为远程客户端分配 IP 地址。如果局域网中配置了 DHCP 服务器，则可由 DHCP 服务器从其地址池中为远程客户分配 IP 地址，否则需要手工设置一个 IP 地址范围，用于分配给远程客户端使用。这里我们选中“自动”单选按钮，单击“下一步”按钮。

(10) 在如图 6-14 所示的“管理多个远程访问服务器”界面中，选中“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮，单击“下一步”按钮。

(11) 系统将开始配置 VPN 服务，配置完成后，将打开如图 6-15 所示的“正在完成路由和远程访问服务器安装向导”界面，单击“完成”按钮。

(12) 在如图 6-16 所示的“配置您的服务器向导”对话框中，单击“完成”按钮。

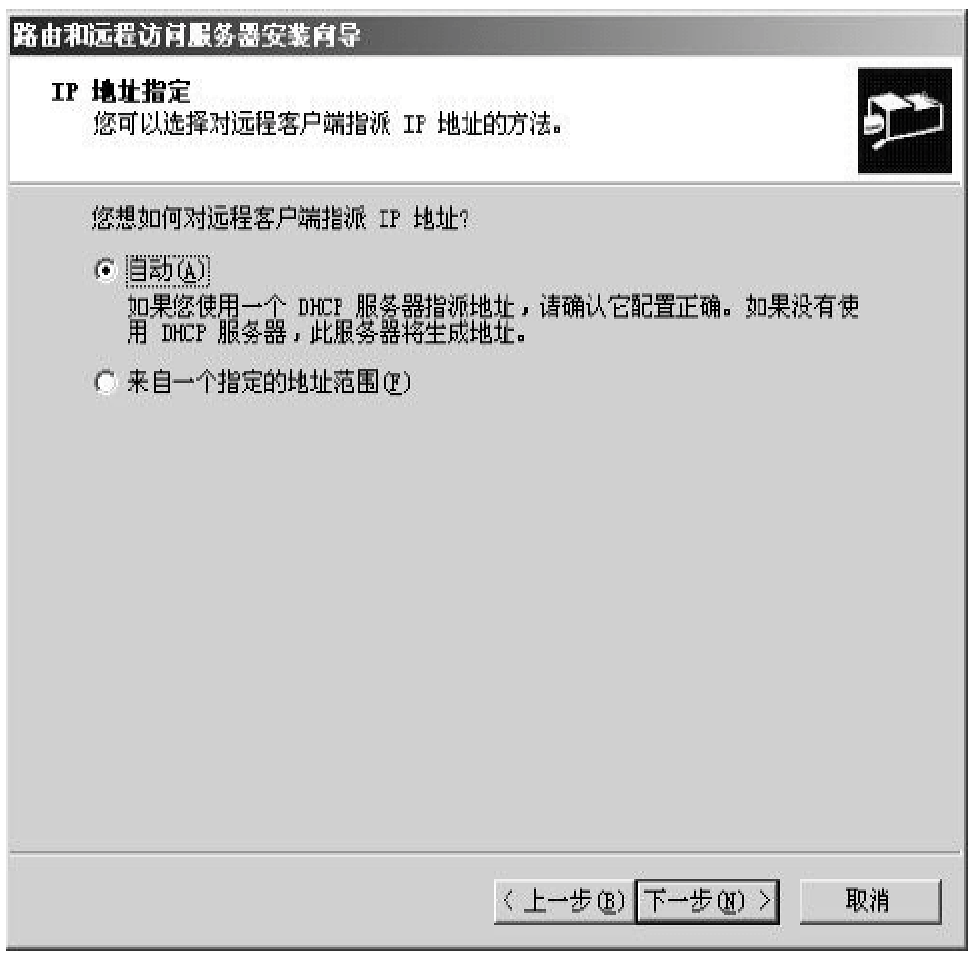


图 6-13　“IP 地址指定”界面

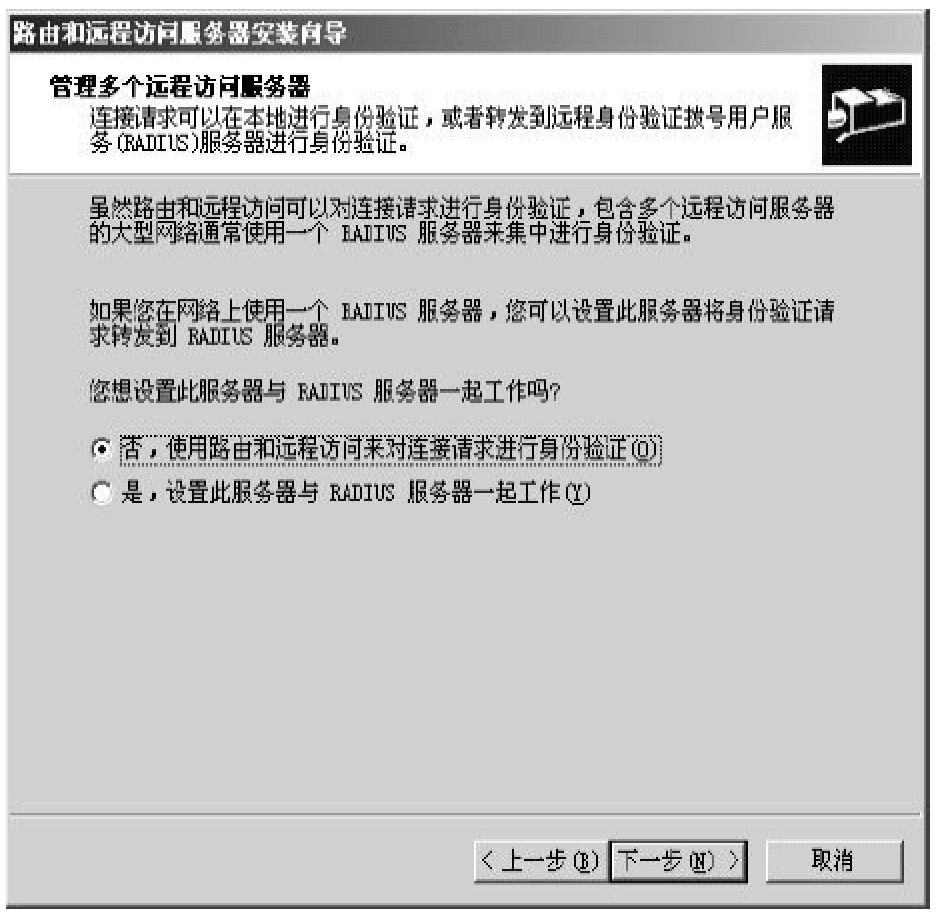
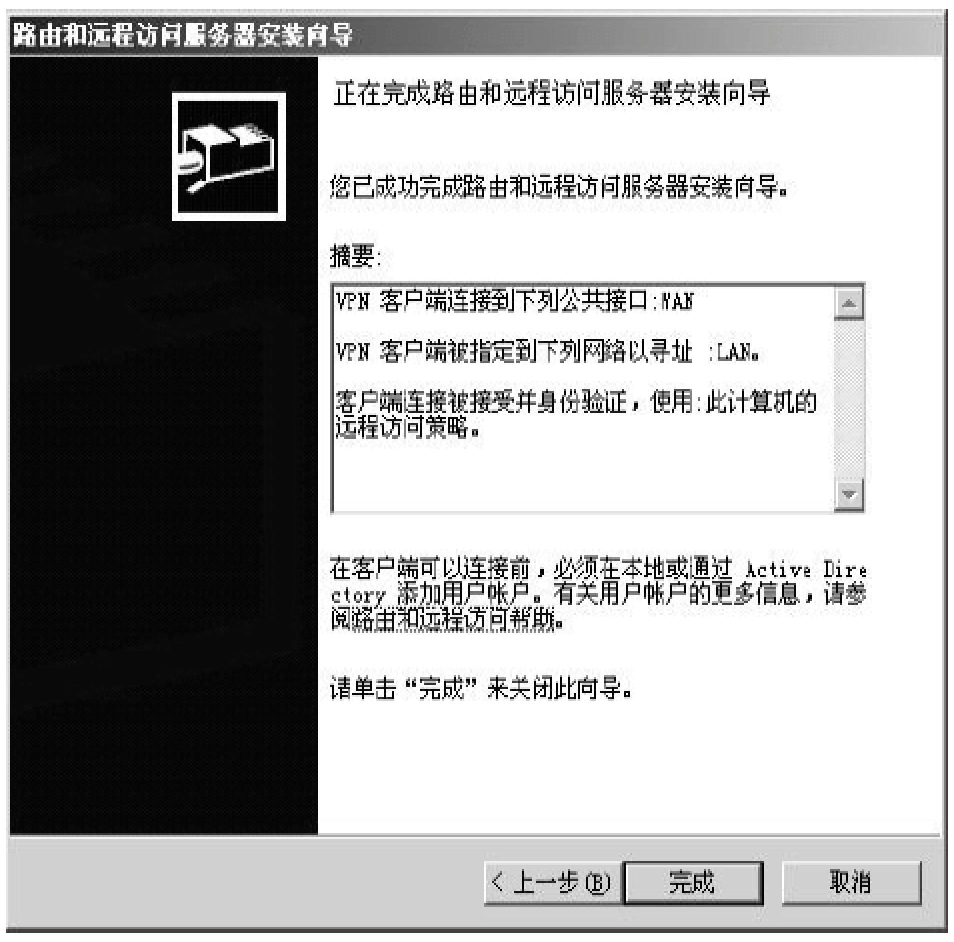


图 6-14　“管理多个远程访问服务器”界面



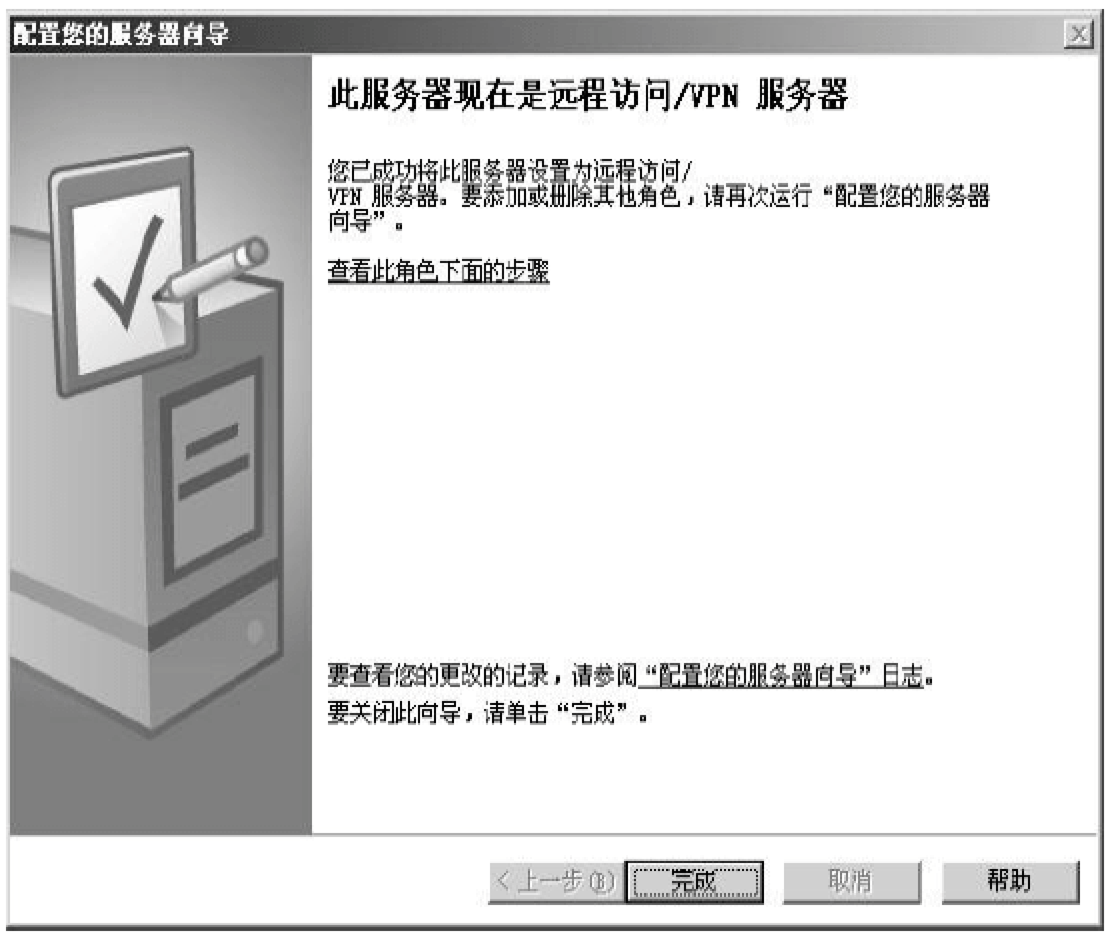


图 6-15　“正在完成路由和远程访问服务器安装向导”界面

图 6-16　VPN 服务器配置完成

VPN 服务器创建完成后，用户可通过依次选择“开始”→“管理工具”命令，运行“路由和远程访问”命令，打开“路由和远程访问”控制台，如图 6-17 所示。在此，用户可对 VPN 服务器进行一些管理和参数的设置。当然，此时即使不做任何额外的设置，VPN 服务器也能正常工作。

2. 添加权限账户

拨入 VPN 服务器需要有一个账号，默认情况下，用户远程访问的权限是被禁止的。

要允许某个用户拥有访问 VPN 服务器的权限，需要在用户的属性对话框中单击“拨入”标签，在“远程访问权限(拨入或 VPN)”选项组中选中“允许访问”单选按钮，以允许该用户通过 VPN 拨入服务器，如图 6-18 所示。

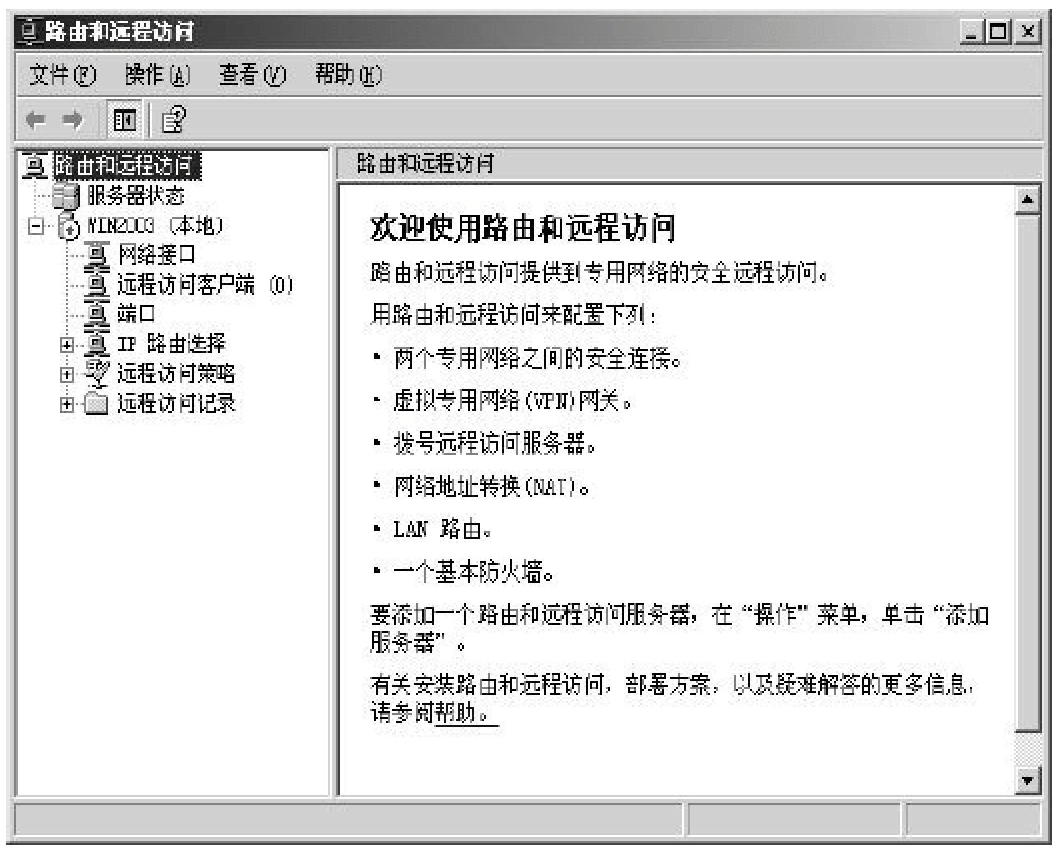


图 6-17 “路由和远程访问”控制台

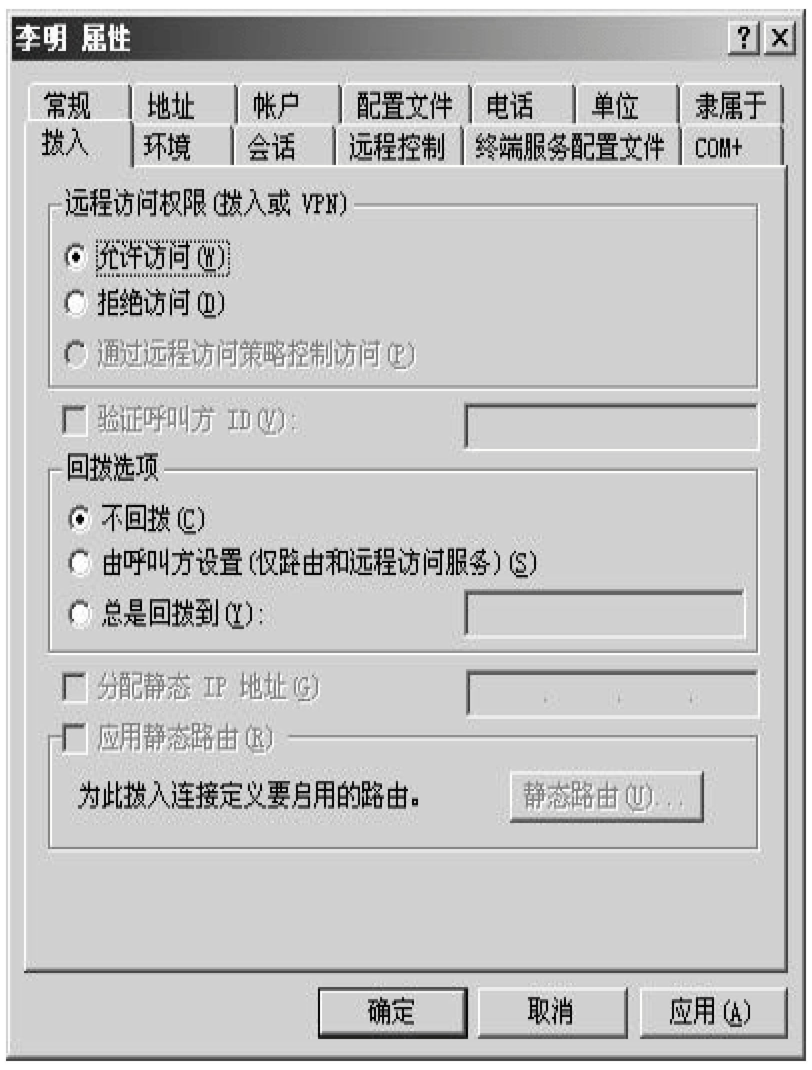


图 6-18 “拨入”选项卡

3. 连接 VPN 服务器

在 Windows XP 上连接 VPN 的操作步骤如下。

(1) 打开“控制面板”窗口，如图 6-19 所示，单击“网络和 Internet 连接”图标。

(2) 在如图 6-20 所示的“网络和 Internet 连接”窗口中，选择“创建一个到您的工作位置的网络连接”选项。

图 6-19 “控制面板”窗口

图 6-20 “网络和 Internet 连接”窗口

(3) 在如图 6-21 所示的“网络连接”界面中选中“虚拟专用网络连接”单选按钮，单击“下一步”按钮。

(4) 在如图 6-22 所示的“连接名”界面中输入连接名称，如公司的名称，单击“下一步”按钮。

(5) 在如图 6-23 所示的“VPN 服务器选择”界面中，输入 VPN 服务器的主机名或者 IP 地址，例如，vpn.example.com，单击“下一步”按钮。

(6) 在如图 6-24 所示的“正在完成新建连接向导”界面中，单击“完成”按钮。

VPN 连接创建完成后，双击桌面上的 VPN 连接图标，在弹出的“连接 example.com”

对话框中输入用户名和密码，如图 6-25 所示，然后单击“连接”按钮，就可以与 VPN 服务器连接上了。

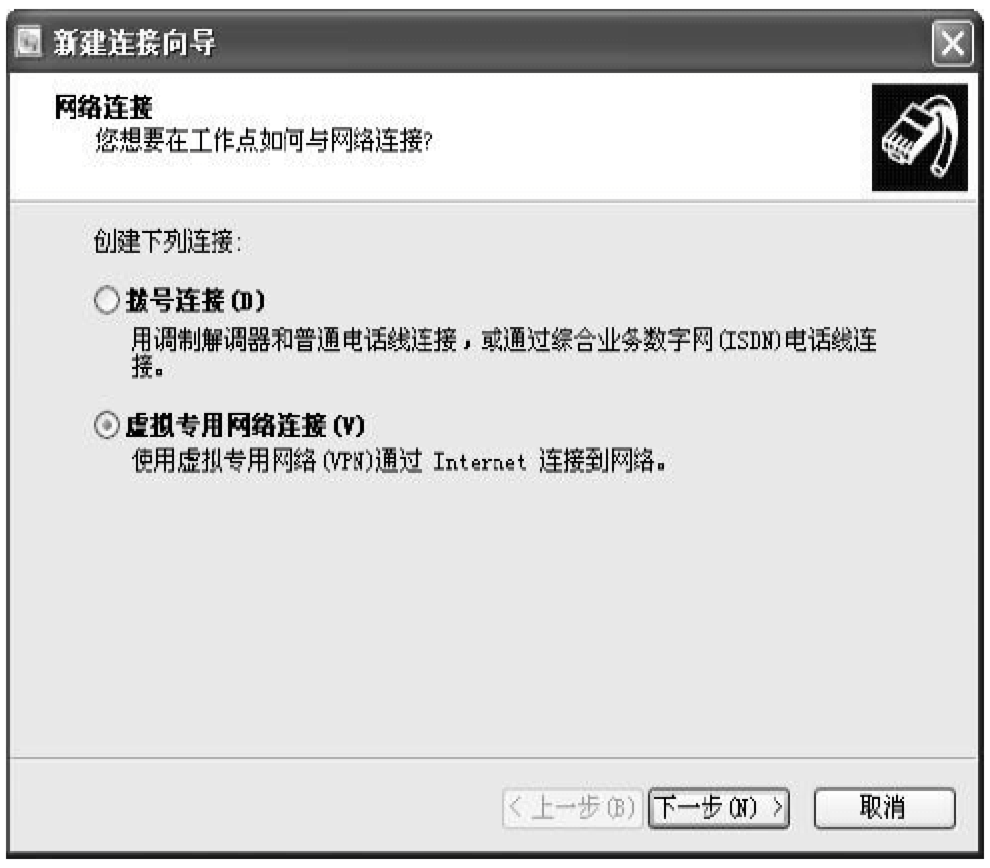


图 6-21　“网络连接”界面

图 6-22　“连接名”界面

图 6-23　“VPN 服务器选择”界面

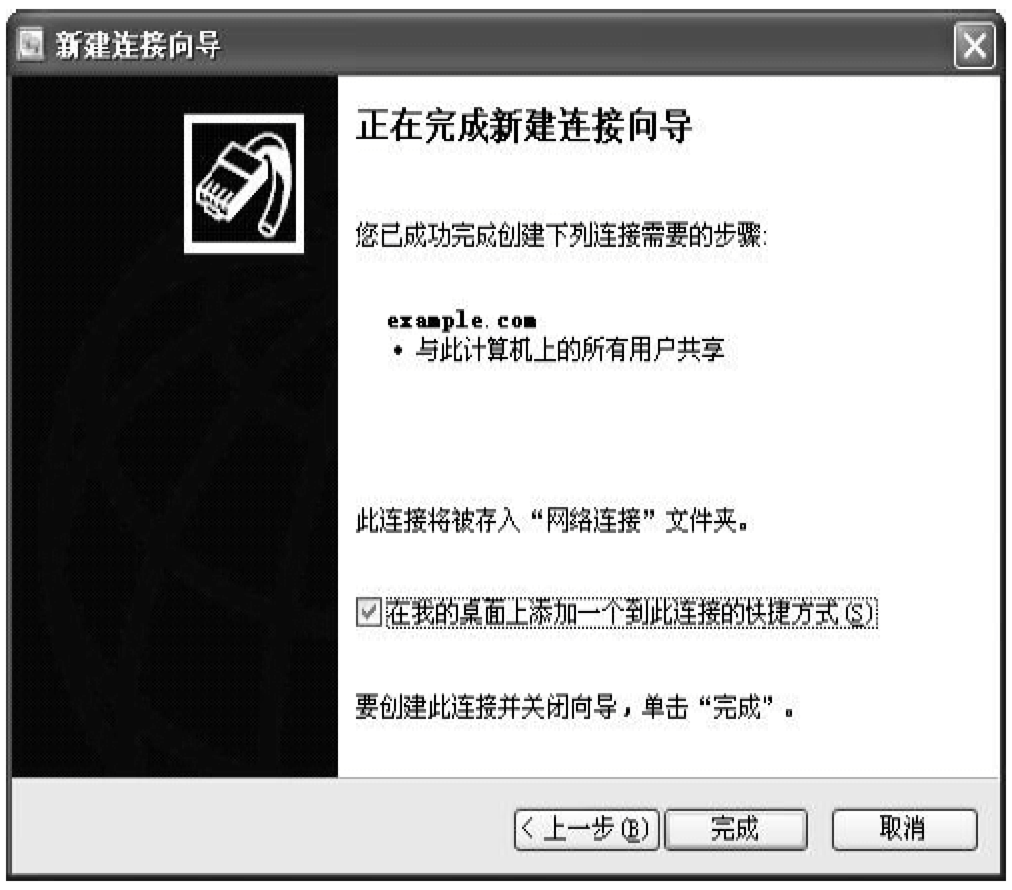


图 6-24　“正在完成新建连接向导”界面

图 6-25　连接 VPN 服务器

6.2.2 典型例题分析

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司有两个办事处，分别利用装有 Windows Server 2008 的双宿主机实现路由功能，此功能由 Windows Server 2008 中的路由和远程访问服务来完成。管理员分别为这两台主机其中一个网卡配置了不同的 IP 地址，如图 6-26 所示。

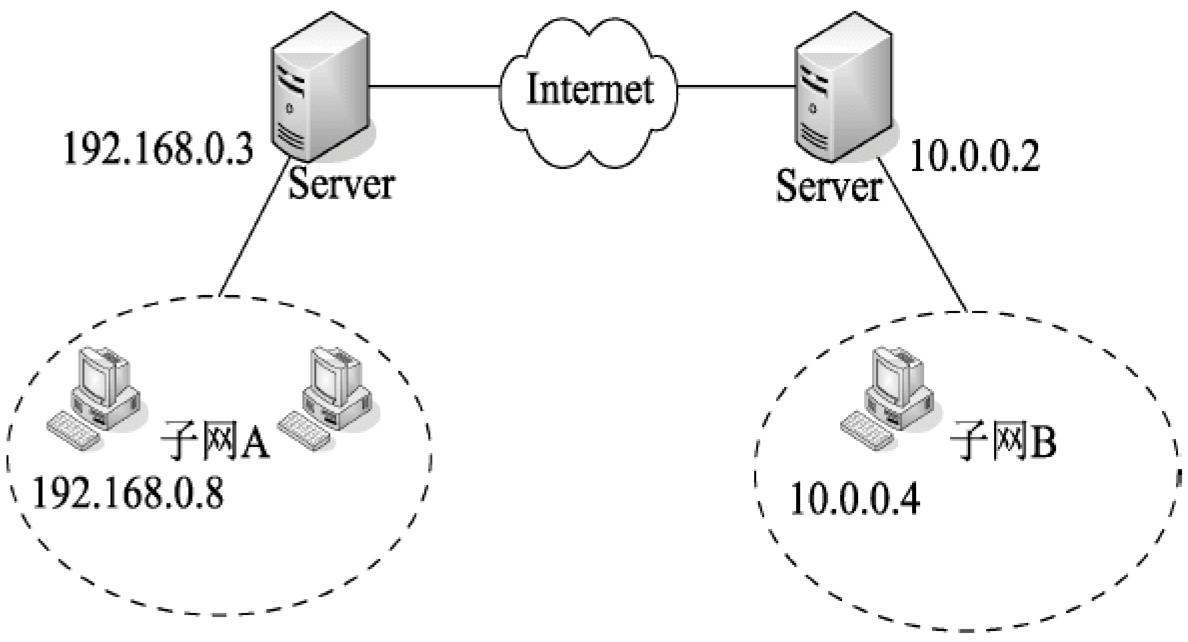


图 6-26 配置 IP 地址

【问题 1】(4 分)

在“管理您的服务器”中单击“添加或删除角色”，此时应当在服务器角色中选择__(1)__来完成路由和远程访问服务的安装。在下列关于路由和远程访问服务的选项中，不正确的是__(2)__。

(1)备选答案：

A. 文件服务器　　B. 应用程序服务器(IIS，ASP.NET)

C. 终端服务器　　D. 远程访问/VPN 服务

(2)备选答案：

A. 可连接局域网的不同网段或子网，实现软件路由器的功能

B. 把分支机构与企业网络通过 Intranet 连接起来，实现资源共享

C. 可使远程计算机接入到企业网络中访问网络资源

D. 必须通过 VPN 才能使远程计算机访问企业网络中的网络资源

【问题 2】(4 分)

两个办事处子网的计算机安装 Windows 7 操作系统，要实现两个子网间的通信，子网 A 和子网 B 中计算机的网关分别为__(3)__和__(4)__。子网 A 中的计算机用 ping 命令来验证数据包能否路由到子网 B 中，图 6-27 中参数使用默认值，从参数__(5)__可以看出数据包经过了__(6)__个路由器。

(3)备选答案：

A. 192.168.0.0　　B. 192.168.0.1　　C. 192.168.0.3　　D. 无须配置网关

(4)备选答案：

A. 10.0.0.0　　B. 10.0.0.1　　C. 10.0.0.2　　D. 无须配置网关

(5)备选答案：

A. bytes　　B. time　　C. TTL　　D. Lost

```
C:\>ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122
Reply from 10.0.0.4: bytes=32 time<10ms TTL=122

Ping statistics for 10.0.0.4:
   Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

图 6-27　参数设置

【问题 3】(8 分)

Windows Server 2008 支持 RIP 动态路由协议。在 RIP 接口属性页中，如果希望路由器每隔一段时间向自己的邻居广播路由表以进行路由信息的交换和更新，则需要在“操作模式”中选择__(7)__。在“传出数据包协议”中选择__(8)__，使网络中其他运行不同版本的邻居路由器都可接受此路由器的路由表；在“传入数据包协议”中选择__(9)__，使网络中其他运行不同版本的邻居路由器都可向此广播路由表。

(7)备选答案：

A. 周期性的更新模式　　B. 自动-静态更新模式

(8)备选答案：

A. RIPv1 广播　　B. RIPv2 多播　　C. RIPv2 广播

(9)备选答案：

A. 只是 RIPv1　　B. 只是 RIPv2

C. RIPv1 和 v2　　D. 忽略传入数据包

为了保护路由器之间的安全通信，可以为路由器配置身份验证。选中“激活身份验证”复选框，并在“密码”文本框中输入一个密码。所有路由器都要做此配置，所配置的密码__(10)__。

(10)备选答案：

A. 可以不同　　B. 必须相同

【问题 4】(4 分)

由于在子网 A 中出现病毒，需在路由接口上启动过滤功能，不允许子网 B 接收来自子网 A 的数据包，在选择入站筛选器且筛选条件是“接收所有除符合下列条件以外的数据包”时，如图 6-28 所示，由源网络 IP 地址和子网掩码得到的网络地址是__(11)__，由目标网络 IP 地址和子网掩码得到的网络地址是__(12)__，需要选择协议__(13)__。如果选择协议__(14)__，则会出现子网 A 和子网 B 之间 ping 不通但是子网 B 能接收来自子网 A 的数据包的情况。

(11)备选答案：

A. 192.168.0.0　　B. 192.168.0.1　　C. 192.168.0.3　　D. 192.168.0.8

(12)备选答案：

A. 10.0.0.0　　B. 10.0.0.1　　C. 10.0.0.3　　D. 10.0.0.4

(13)～(14)备选答案：

A. ICMP　　B. TCP　　C. UDP　　D. 任何

图 6-28 “添加 IP 筛选器”对话框

答案:

【问题 1】(1) D (2) D

【问题 2】(3) C (4) C (5) C (6) 133

【问题 3】(7) A (8) A (9) C (10) B

【问题 4】(11) A (12) D (13) D (14) A

解析:

【问题 1】在 Windows 系统中，要想实现路由和远程访问服务需要以管理员身份登录，打开“控制面板”窗口，运行“添加和删除程序”命令，选择“添加或删除 Windows 组件”，启动 Windows 组件向导，选择“远程访问/VPN 服务”即可。

针对普通用户的远程访问需求，较为常见的方式有 3 类。

第一类是直接开放内部应用系统的端口，允许外部 IP 直接访问，通过应用系统自身的账号验证机制防范非法用户。

第二类是利用 Windows Server 2003 及更新的版本所提供的 Terminal Service 功能，在外部 PC 上运行 Windows 远程桌面，先连接到内网的 Terminal Server，再通过该 Server 代理访问内网应用系统。

第三类是采用 VPN 技术实现与企业内网的远程连接，进而在 VPN 中访问内网应用系统。因此 VPN 并不是远程计算机访问企业网络的唯一途径，并不是必须通过 VPN。

【问题 2】ping 命令通常用于测试连通性。同时，ICMP 回答报文中的 TTL 代表的跳数，从 255 跳开始，每经过一个路由器，TTL 值减 1，由图 6-27 可知 TTL=122，故已经过 255−122 =133 跳。

【问题 3】为支持 RIP 动态路由协议，可自己相应配置，RIP 有两个版本，V1 只支持有类路由信息，并以广播的形式发送整个路由表给邻居；V2 支持无类别路由，以组播的方式发送整个路由表信息进行路由收敛。

【问题 4】出现两个网络之间 ping 不通但是其中一个网络能接收来自另一个网络的数据包的情况，一般是采用了 ICMP 协议，ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。

6.2.3　同步练习

1. 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2014 年 5 月试题四)

【说明】

某企业总部设立在 A 地，在 B 地有分支机构，分支机构和总部需要在网络上进行频繁的数据传输。该企业采用 IPSec VPN 虚拟专用技术实现分支机构和总部直接的安全、快捷、经济的跨区域网络连接。

该企业网络拓扑结构如图 6-29 所示。

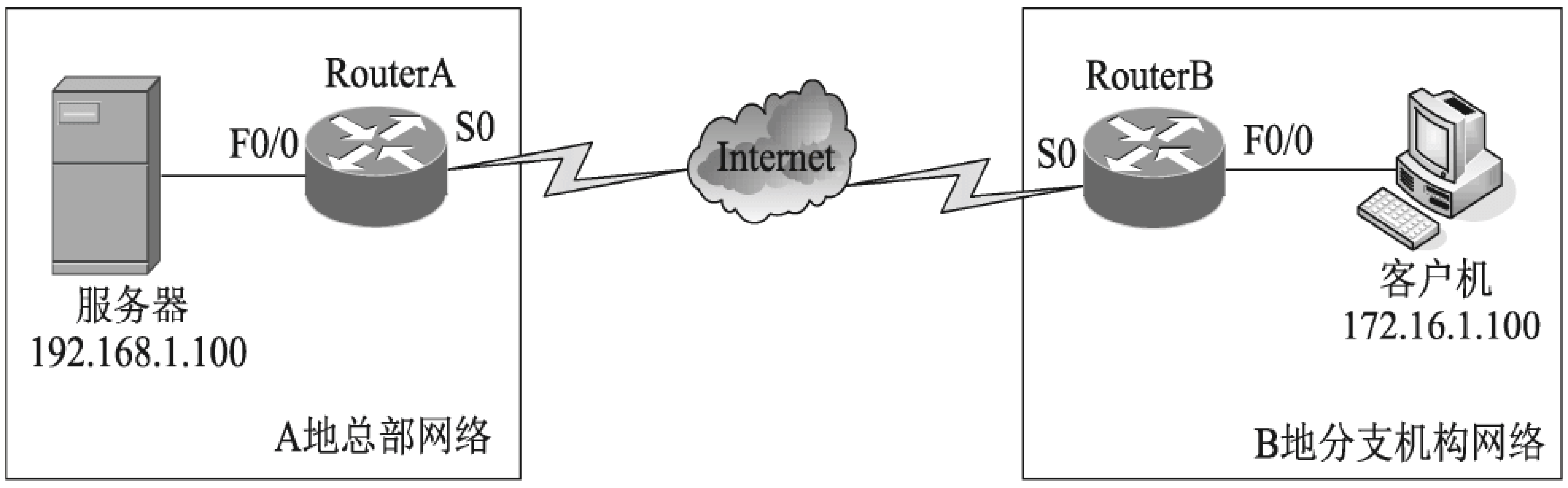


图 6-29　网络拓扑结构图

该企业的网络地址规划及配置如表 6-5 所示。

表 6-5　网络规划地址配置表

设　备	IP 地址	设　备	IP 地址
RouterA	F0/0: 172.16.1.1/24 S0:202.102.100.1/30	RouterB	F0/0:192.168.1.1/24 S0:202.102.100.2/30
总部服务器	192.168.1.100/24	分支机构客户端	172.16.1.100/24

【问题 1】(7 分)

为了完成对 RouterA 和 RouterB 远程连接管理，以 RouterA 为例，完成初始化路由器，并配置 RouterA 的远程管理地址(192.168.1.20)，同时开启 RouterA 的 Telent 功能并设置全局模式访问密码，请补充下列配置命令。

```
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface f0/0  //进入 F0/0 的 (1) 子模式
RouterA(config-if)#ip addr  (2)  //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut  // (3) F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter (4) //进入 lookback0 的接口配置子模式
RouterA(config-if)#ip addr (5) //为 loopback0 接口配置 IP 地址
RouterA(config)# (6) //进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001//配置 vty 口令为“abc001”
RouterA(config)#enable password abc001//配置全局配置模式的明文密码为“abc001”
RouterA(config)#enable (7) abc001//配置全局配置模式的密文密码为“abc001”
```

【问题 2】(5 分)

VPN 是建立在两个局域网出口之间的隧道链接，所以两个 VPN 设备必须能够满足内外访问互联网的要求，以及需要配置 NAT，按照题目要求，以 RouterA 为例，请补充完成下列配置命令。

```
RouterA(config)#access-list 101 __(8)__ ip 192.168.1.0  0.0.0.255  172.16.1.0
0.0.0.255
RouterA(config)#access-list 101 __(9)__ ip 192.168.1.0  0.0.0.255 any
//定义需要被 NAT 的数据流
RouterA(config)#ip nat inside sourcelist 101 interface __(10)__ overload
//定义 NAT 转换关系
RouterA(config)#int __(11)__
RouterA(config-if)#ip nat inside
RouterA(config)#int __(12)__
RouterA(config-if)#ip nat outside //定义 NAT 的内部和外部
```

【问题 3】(4 分)

配置 IPSec VPN 时，要注意隧道两端的设备配置参数必须对应匹配，否则 VPN 配置将会失败，以 RouterB 为例，配置 IPSec VPN，请完成相关配置命令。

```
RouterB(config)#access-list 102 permit ip __(13)__
//定义需要经过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp __(14)__   //启用 ISAKMP(IKE)
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#group 2
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address __(15)__
//指定共享密钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp_md5_hmac
RouterB(cfg-crypto-trans)#model tunnel
RouterB(config)#crypto map abc001 10 ipsec-isakmp
RouterB(config)#int __(16)__
RouterB(config)-if)#crypto map abc001  //在外部接口上应用加密图
```

【问题 4】

根据题目要求，企业分支机构与总部之间采用 IPSec VPN 技术互联，IPSec(IP Security)是 IETE 为保证在 Internet 上传输数据的安全性、保密性而制定的框架协议。该协议使用在(17)层，用于保证和认证用户 IP 数据包。

IPSec VPN 可使用的模式有两种，其中 (18) 模式的安全性较强， (19) 模式的安全性较弱。IPSec 主要由 AH/ESP 和 IKE 组成。在使用 IKE 协议时，需要定义 IKE 协商策略。该策略由 (20) 进行定义。

2. 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】 某企业在部门 A 和部门 B 分别搭建了局域网，两局域网通过两台 Windows Server 2003 服务器连通，如图 6-30 所示，要求采用 IPSec 安全机制，使得部门 A 的主机 PC1

可以安全访问部门 B 的服务器 S1。

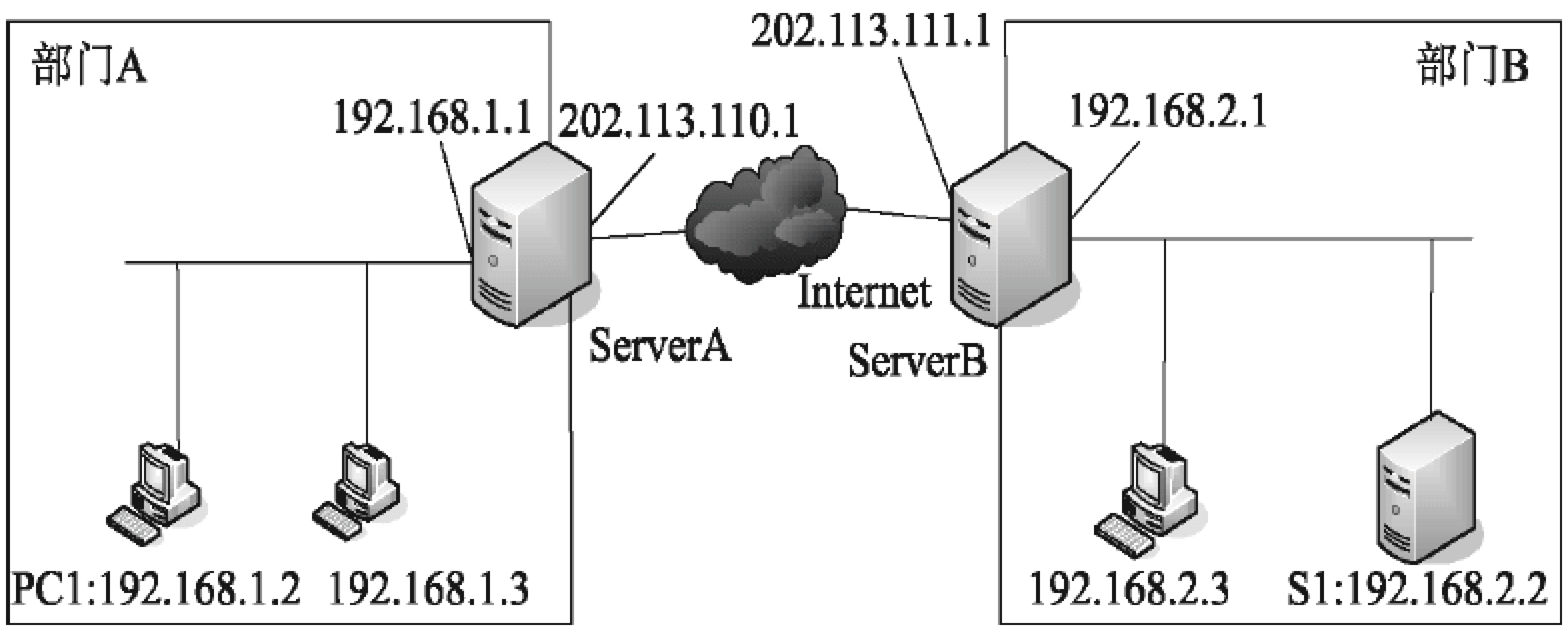


图 6-30　局域网结构图

【问题 1】(3 分，每空 1 分)

IPSec 工作在 TCP/IP 协议栈的 (1) 层，为 TCP/IP 通信提供访问控制、数据完整性、数据源验证、抗重放攻击、机密性等多种安全服务。IPSec 包括 AH、ESP 和 ISAKMP/Oakley 等协议，其中， (2) 为 IP 包提供信息源和报文完整性验证，但不支持加密服务； (3) 提供加密服务。

【问题 2】(2 分)

IPSec 支持传输和隧道两种工作模式，如果要实现 PC1 和 S1 之间端到端的安全通信，则应该采用 (4) 模式。

【问题 3】(6 分，每空 2 分)

如果 IPSec 采用传输模式，则需要在 PC1 和 (5) 上配置 IPSec 安全策略。在 PC1 的 IPSec "IP 筛选器 属性"对话框(见图 6-31)中，源 IP 地址应设为 (6) ，目标 IP 地址应设为 (7) 。

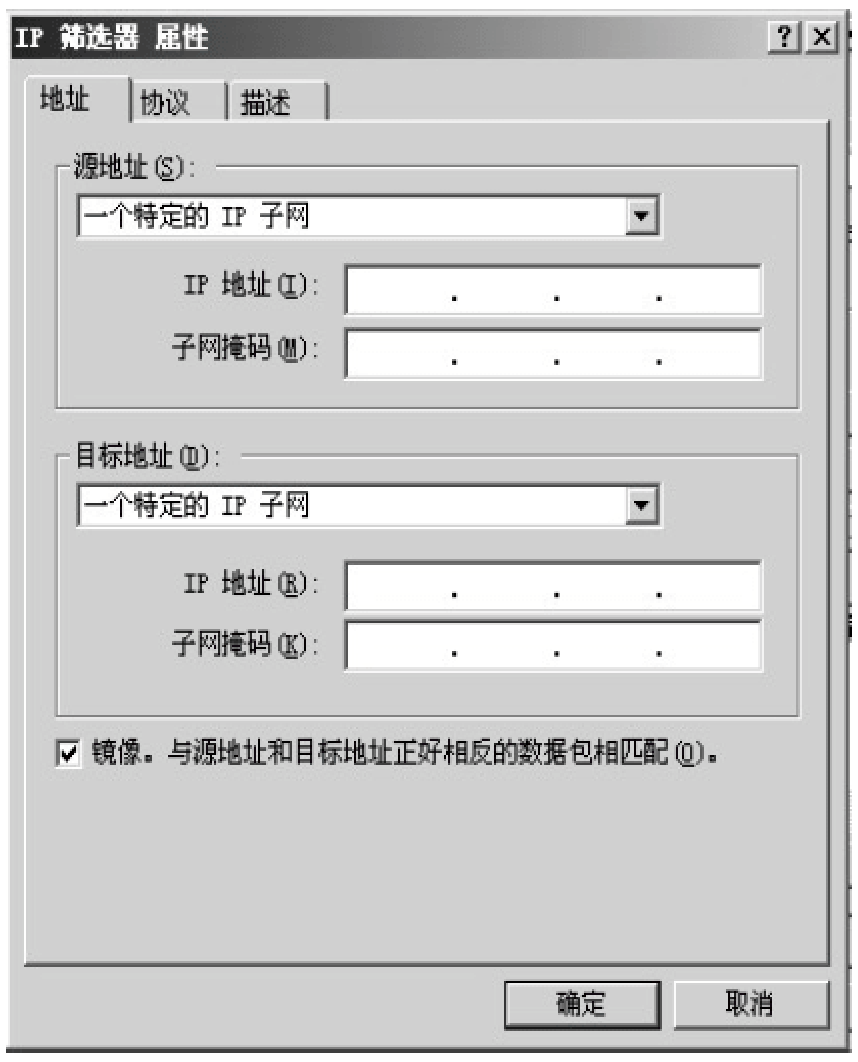


图 6-31　"IP 筛选器 属性"对话框

【问题 4】(4 分，每空 1 分)

如果要保护部门 A 和部门 B 之间所有的通信安全，则应该采用隧道模式，此时需要在 ServerA 和 (8) 上配置 IPSec 安全策略。在 ServerA 的"IP 筛选器 属性"对话框中(见图 6-32)，源 IP 子网的 IP 地址应设为 (9) ，目标子网 IP 地址应设为 (10) ，源地址和目标地址的子网掩码均设为 255.255.255.0。ServerA 的 IPSec 规则设置中(见图 6-33)，指定的隧道端点 IP

地址应设为 (11) 。

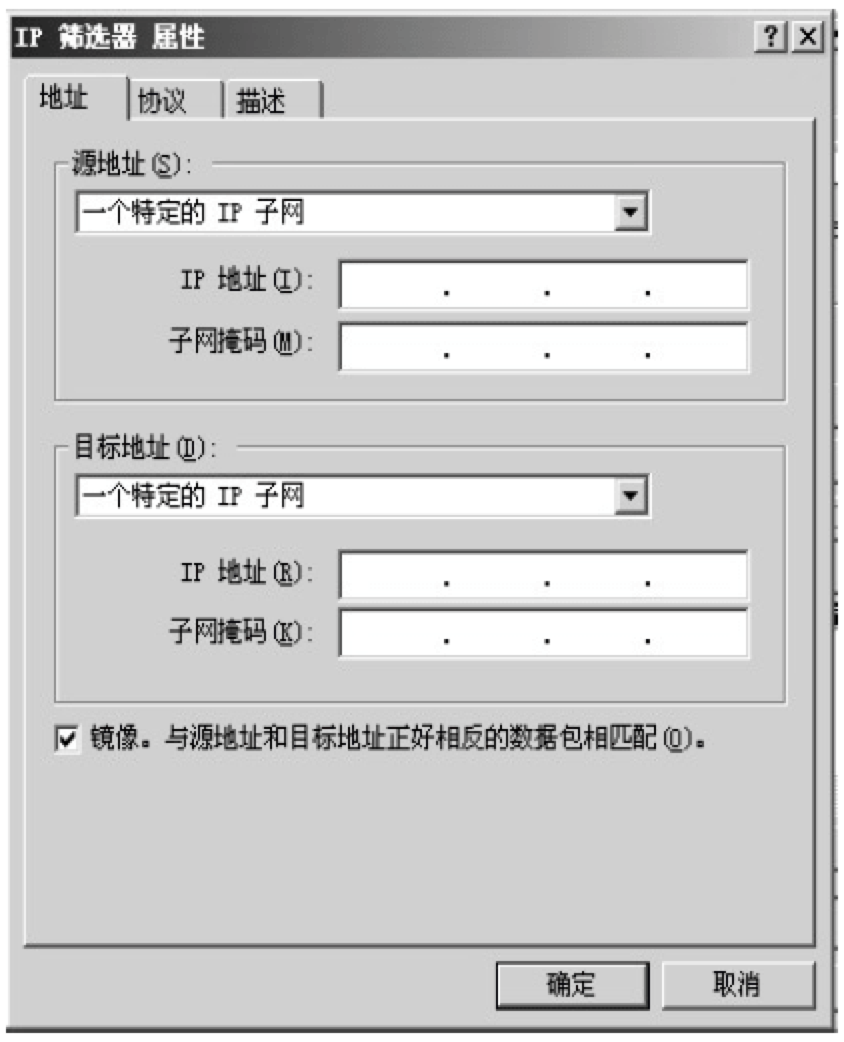


图 6-32　子网 IP 地址的设置

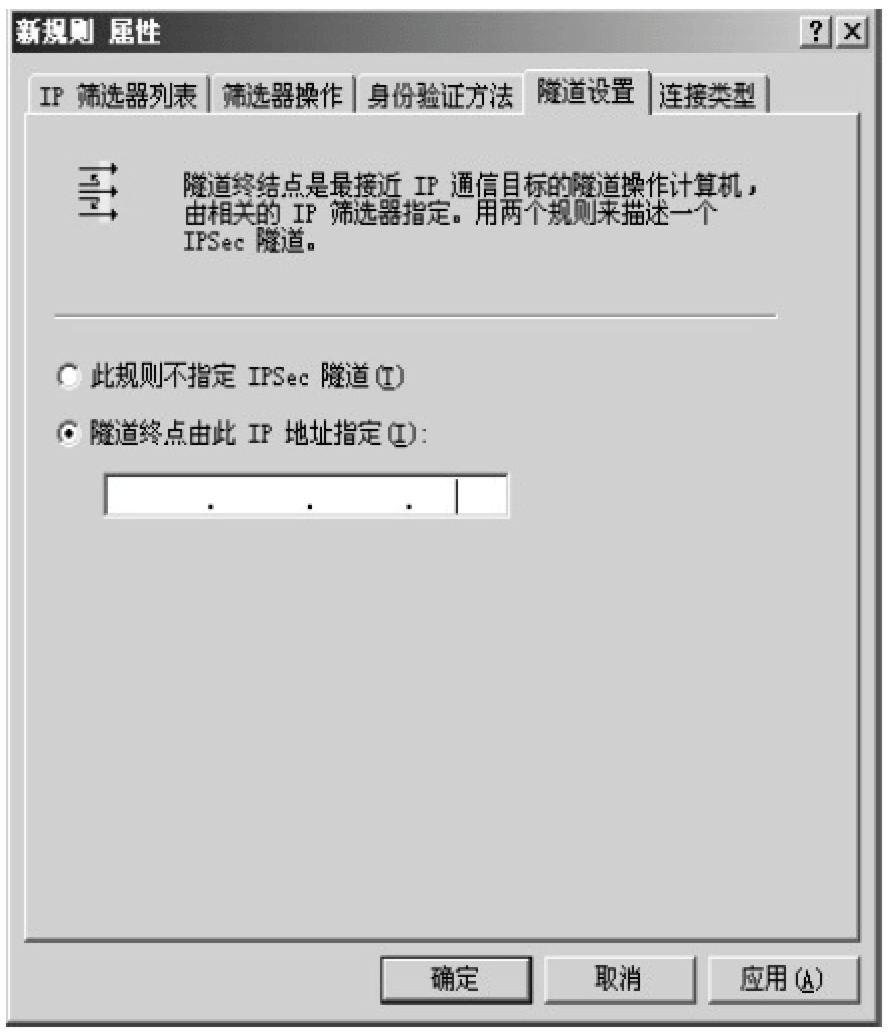


图 6-33　IPSec 规则设置

3. 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】 某企业在公司总部和分部之间采用两台 Windows Server 2003 服务器部署企业 IPSec VPN，将总部和分部的两个子网通过 Internet 互联，如图 6-34 所示。

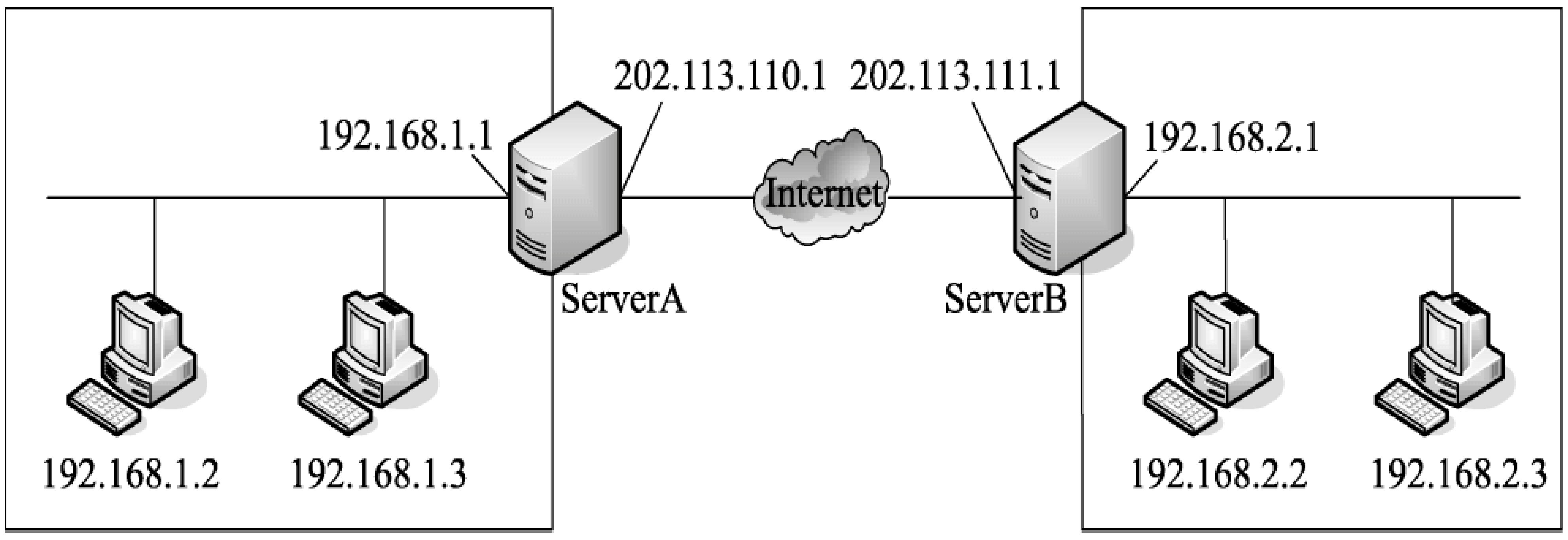


图 6-34　总部和分部连接图

【问题 1】(3 分)

隧道技术是 VPN 的基本技术，隧道是由隧道协议形成的，常见隧道协议有 IPSec、PPTP 和 L2TP。其中 (1) 和 (2) 属于第二层隧道协议， (3) 属于第三层隧道协议。

【问题 2】(3 分)

IPSec 安全体系结构包括 AH、ESP 和 ISA KMP/Oakley 等协议。其中， (4) 为 IP 包提供信息源验证和报文完整性验证，但不支持加密服务； (5) 提供加密服务； (6) 提供密钥管理服务。

【问题 3】(6 分)

设置 ServerA 和 ServerB 之间通信的筛选器属性界面，如图 6-35 所示，在 ServerA 的 IPSec 安全策略配置过程中，当源地址和目标地址均设置为“一个特定的 IP 子网”时，源子网 IP 地址应设为 (7) ，目标子网 IP 地址应设为 (8) 。图 6-36 所示的隧道设置中的隧道终点 IP 地址应设为 (9) 。

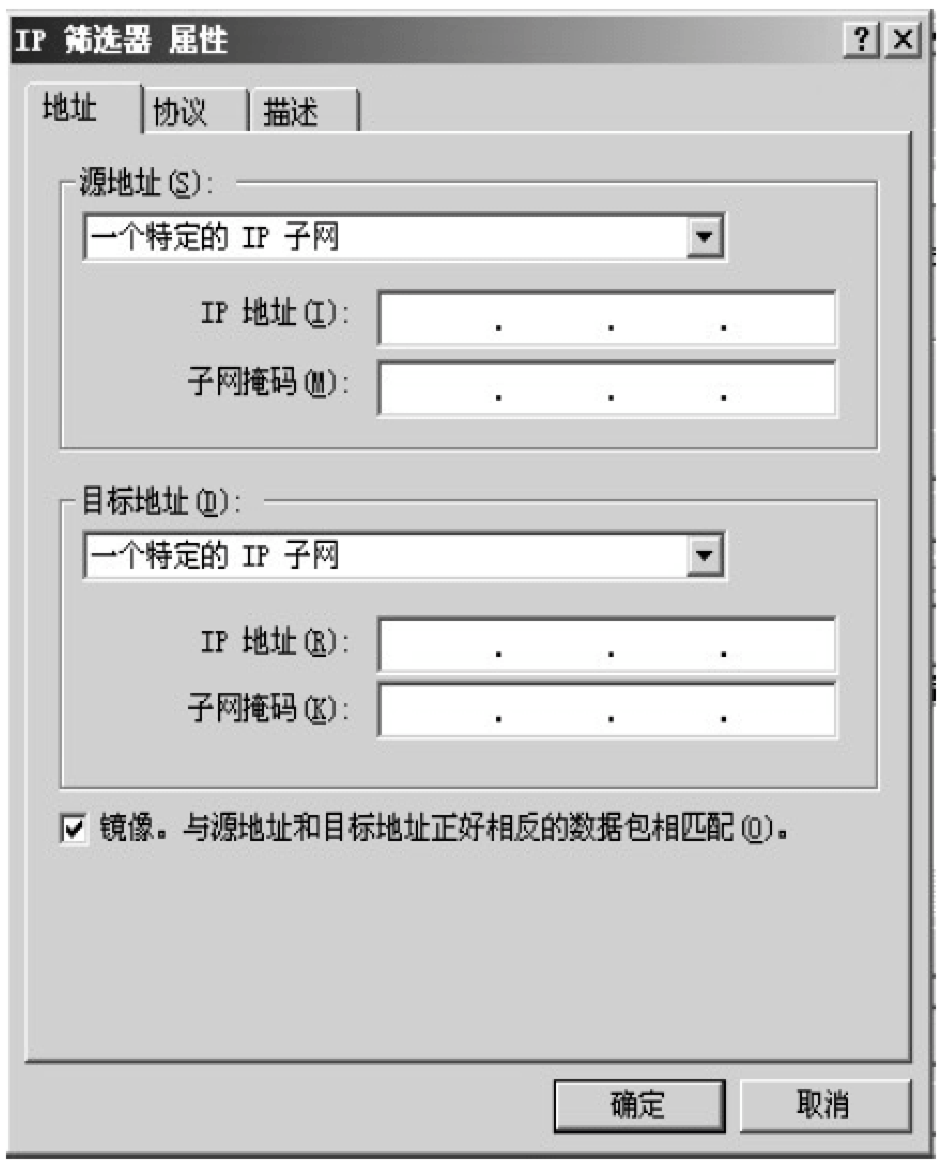


图 6-35　"IP 筛选器 属性"对话框

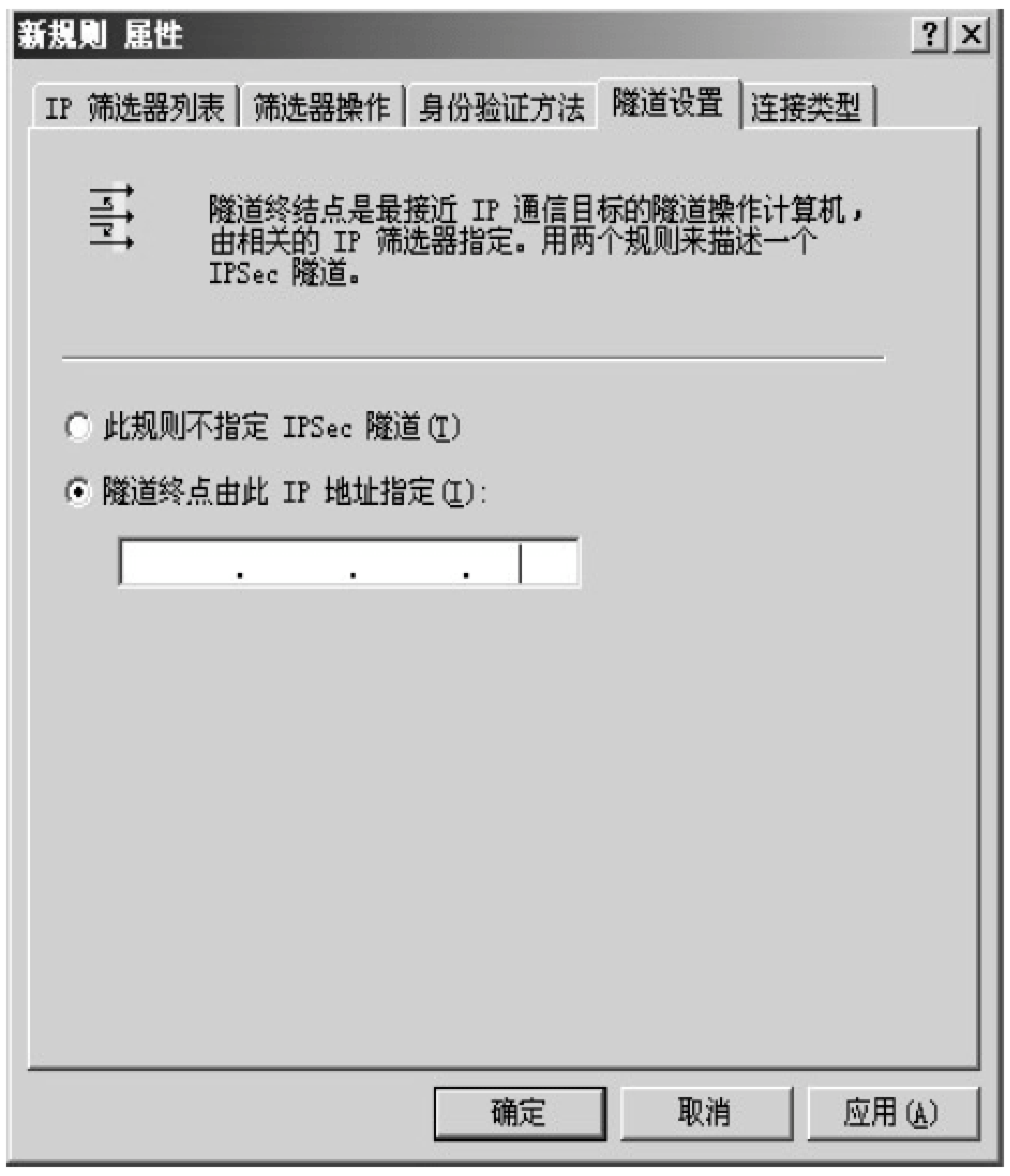


图 6-36　隧道设置

【问题 4】(3 分)

在 ServerA 的 IPSec 安全策略配置过程中，ServerA 和 ServerB 之间通信的 IPSec 筛选器安全设置为"协商安全"，并且安全措施为"加密并保持完整性"，如图 6-37 所示。根据上述安全策略填写图 6-38 中的空格，表示完整的 IPSec 数据包格式。

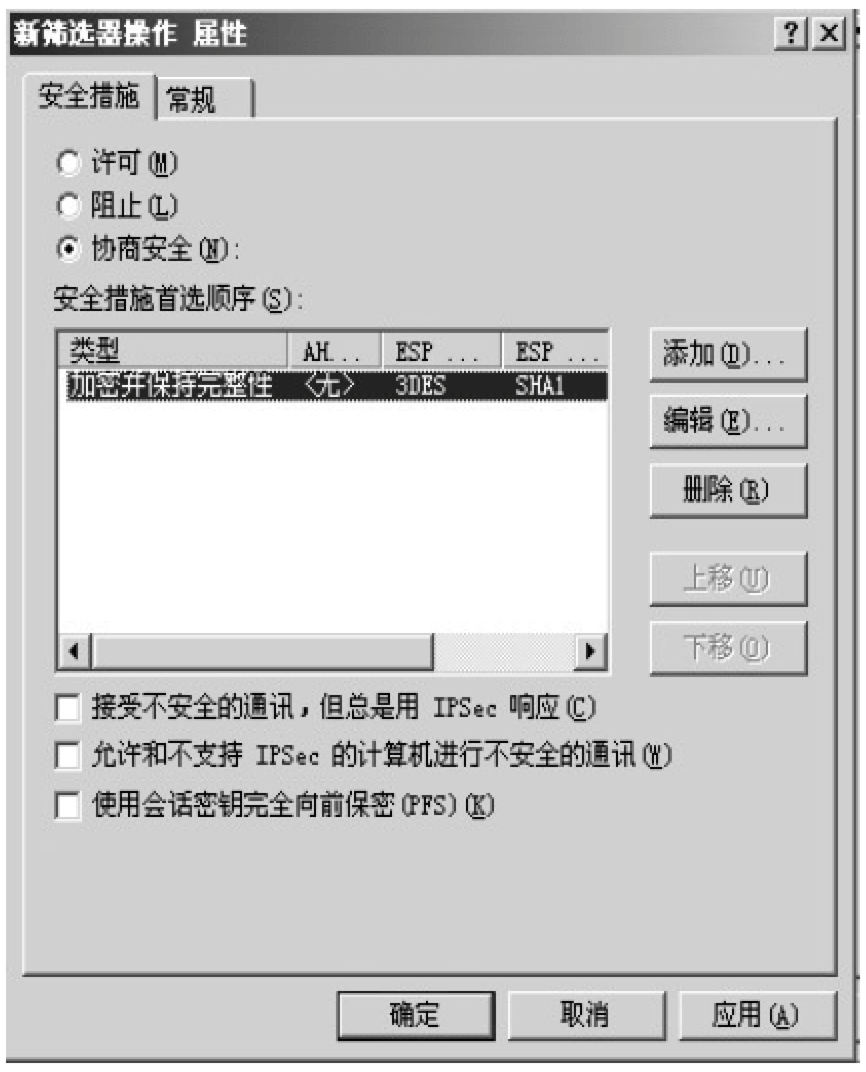


图 6-37　"新筛选器操作 属性"对话框

新 IP 头	(10)	(11)	TCP 头	数据	(12)

图 6-38　IPSec 数据包格式

(10)～(12)备选答案：

A. AH 头　　B. ESP 头　　C. 旧 IP 头　　D. 新 TCP 头

E. AH 尾　　F. ESP 尾　　G. 旧 IP 尾　　H. 新 TCP 尾

6.2.4 同步练习参考答案

1. 答案：

【问题 1】

(1) 接口配置或端口配置　(2) 192.168.1.1 255.255.255.0　(3) 激活　(4) lookback 0

(5) 192.168.1.20　255.255.255.255　(6) line vty0 4　(7) secret

【问题 2】

(8) deny　(9) permit　(10) S0　(11) F0/0　(12) S0

【问题 3】

(13) 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255　(14) enable

(15) 202.102.100.1　(16) S0

【问题 4】

(17) 网络层　(18) 隧道　(19) 传输　(20) ISAKMP/Oakley

解析：

【问题 1】

RouterA>enable

RouterA#configure terminal

RouterA(config)#interface F0/0　//进入 F0/0 的接口配置子模式

RouterA(config-if)#ip addr 192.168.1.1　255.255.255.0　//为 F0/0 接口配置 IP 址

RouterA(config-if)#no shut　//激活 F0/0 接口，默认所有路由器的接口都为 down 状态

RouterA(config-if)#inter loopback 0　//进入 lookback0 接口配置子模式

RouterA(config-if)#ip addr 192.168.1.20　255.255.255.255 //为 lookback0 接口配置 IP 地址

RouterA(config)#line vty0 4　//进入虚拟接口 0-4 的配置子模式

RouterA(config-line)#password abc001　//配置 vty 口令为“abc001”

RouterA(config)#enable password abc001　//配置全局配置模式的明文密码为“abc001”

RouterA(config)# enable secret abc001　//配置全局配置模式的密文密码为“abc001”

【问题 2】

RouterA(config)#access-list 101 deny ip 192.158.1.0　0.0.0.255　172.15.1.0　0.0.0.255

//拒绝来自 192.168.1.0/24 去往 172.16.1. 0/24 网络的流量

RouterA(config)#access-list 101 permit ip 192.168.1.0　0.0.0.255 any

//定义要被 NAT 的数据流

RouterA(config)#ip nat inside source list 101 interface S0 overload

//NAT 转换关系(匹配 ACL101 的数据流都翻译成 S0 接口的公网 IP 地址，此为地址伪装)

RouterA(config)#int F0/0

RouterA(config-if)#ip nat inside　//定义 NAT 的内部接口

RouterA(config)#int S0

RouterA(config-if)#ip nat outside　//定义 NAT 的外部接口

【问题 3】

RouterB(config)#access-list 102 permit ip 172.15.1.0 0.0.0.255 192.168.1.0 0.0.0.255
//定义要通过 VPN 加密传输的数据流

RouterB(config)#crypto isakmp enable　//启用 ISAKMP(IKE)

RouterB(config)#crypto isakmp policy 10　//建立 IKE 协商策略

RouterB(config-isakmp)#authentication pre-share　//使用预定义密钥

RouterB(config-isakmp)#encryption des　//加密算法

RouterB(config-isakmp)#hashmd5　//HASH 算法

RouterB(config-isakmp)#group2　//设置 1024 位 Diffie-Hellman 非对称加密算法

RouterB(config)#crypto isakmp identity address
//指定 ISAKMP 与分部路由器进行身份认证时使用 IP 地址作为标志

RouterB(config)#crypto isakmp key abc001 address 202.102.100.1
//指定共享密钥和对端设备地址

RouterB(config)#crypto ipsect ransform-set ccie esp-des esp-md5-hmac
//配置 ipsec 交换集模式

RouterB(cfgcrypto-trans)#model tunnel　//配置隧道模式

RouterB(config)#crypto map abc001 10 ipsec-isakmp　//配置加密图

RouterB(config)#int S0

RouterB(config-if)#crypto map abc001　//在外部接口上应用加密图

【问题 4】

Internet 协议安全性(IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议(IP)网络上进行保密而安全地通信。

IPSec 协议工作在 OSI 模型的第三层(网络层)使其在单独使用时适于保护基于 TCP 或 UDP 的协议(如安全套接子层(SSL)就不能保护 UDP 层的通信流)。

IPSec VPN 可使用的模式有两种：隧道模式和传输模式。

隧道(tunnel)模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通信。

传输(transport)模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放在原 IP 数据包后面。通常，传输模式应用在两台主机之间的通信，或一台主机和一个安全网关之间的通信。

二者相对而言，隧道模式安全性高于传输模式。

在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由 ISAKMP/Oakley 进行定义。

2. **答案：**

【问题 1】

(1) 网络　(2) AH　(3) ESP

【问题 2】

(4) 传输

【问题 3】

(5) S1　(6) 192.168.1.2　(7) 192.168.2.2

【问题 4】

(8) ServerB　(9) 192.168.1.0　(10) 192.168.2.0　(11) 202.113.111.1

解析：

【问题 1】IPSec(Security Architecture for IP Network，IP 层协议安全结构)工作在 TCP/IP 协议栈的网络层。IPSec 认证头(AH)提供了数据完整性和数据源认证，但不提供保密服务；IPSec 封装安全负荷(ESP)提供了数据加密功能，它利用对称密钥对 IP 数据进行加密。

【问题 2】 IPSec 提供了两种模式，即传输模式和隧道模式。在传输模式中，IPSec 认证头(AH)或 IPSec 封装安全负荷(ESP)头插入原来的 IP 头之后；而在隧道模式中，IPSec 用新的 IP 头封装了原来的 IP 数据报。

【问题 3】 由图 6-30 可知，在 PC1 和 S1 上配置安全策略，源 IP 地址即 PC1 的 IP 地址 192.168.1.2，目标 IP 地址即 S1 的 IP 地址 192.168.2.2。

【问题 4】 由图 6-30 可知，采用隧道模式需要在 ServerA 和 ServerB 上配置安全策略，源 IP 子网的 IP 地址，(9)和(10)分别是 ServerA 和 ServerB 所对应的网段 IP 地址，分别为 192.168.1.0 和 192.168.2.0，隧道端点 IP 地址如图 6-30 所示为 202.113.111.1。

3. **答案：**

【问题 1】

(1) PPTP　(2) L2TP　(3) IPSec

说明：(1)和(2)答案可调换。

【问题 2】

(4) AH　(5) ESP　(6) ISAKMP/Oakley

【问题 3】

(7) 192.168.1.0　(8) 192.168.2.0　(9) 202.113.111.1

【问题 4】

(10) B　(11) C　(12) F

解析：

【问题 1】本题考查 VPN 隧道技术的基本概念，这里不作详细的解析。

【问题 2】本题考查 IPSec 协议组的功能。

【问题 3】源子网 IP 地址为 ServerA 连接的内网网络地址，由图 6-34 可知为 192.168.1.0；目标子网 IP 地址应为 ServerB 连接的内网网络地址，由图 6-34 可知为 192.168.2.0。

隧道设置中的隧道终点 IP 地址应设置为服务器 ServerB 的外网地址，为 202.113.111.1。

【问题 4】题目中要求安全措施为“加密并保持完整性”。IPSec 封装安全负荷(ESP)提供了数据加密功能和数据完整性认证。在隧道模式下，IPSec 对原来的 IP 数据报进行了封装和加密，加上了新的 IP 头，其格式如下。

新IP头	ESP头	原来的IP头	TCP头	数据	ESP尾

6.3 病 毒 防 护

6.3.1 考点辅导

6.3.1.1 计算机病毒

所谓病毒是指一段可执行的程序代码，它通过对其他程序进行修改，来感染这些程序使其含有该病毒程序的一个复制。病毒可以做其他程序所做的任何事，唯一的区别在于它将自己附在另一个程序上，并且在宿主程序运行时秘密执行。一旦病毒执行时，它可以完成任何功能，例如删除文件和程序等。

大多数病毒按照一种与特定操作系统有关的，或者在某种情况下，与特定硬件平台有关的方式来完成它们的工作。因此，它们可以被设计成利用特定系统的细节和漏洞工作。

6.3.1.2 病毒的类型

计算机病毒的分类有很多种，最常见的分类方法是按照寄生方式和传染途径分类。计算机病毒按其寄生方式大致可分为两类：一是引导型病毒；二是文件型病毒，混合型病毒集这两种病毒特性于一体。

1. 引导型病毒

引导型病毒会去感染磁盘上引导扇区的内容(软盘或硬盘都有可能感染病毒)，或者改写硬盘上的分区表(FAT)。如果用启动已感染病毒的软盘的话，则会感染硬盘。

2. 文件型病毒

文件型病毒主要以感染文件扩展名为.com、.exe 和.vol 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存。已感染病毒的文件执行速度会减缓，甚至无法执行。有些文件遭感染后，一执行就会遭到删除。

3. 宏病毒

宏病毒(文件型病毒的一种)是一种寄存于文档或模板(Word 或 Excel)的宏中的计算机病毒。一旦打开被感染的文档，宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会被感染上这种病毒，如果其他用户打开了感染病毒的文档，病毒就会转移到其他计算机上。

4. 混合型病毒

混合型病毒综合引导型病毒和文件型病毒的特性，它的破坏性也比引导型和文件型病毒更强。这种病毒通过这两种方式来感染，更增加了病毒的传染性以及存活率。不管以哪种方式传染，计算机只要中毒就会在开机或执行程序时感染其他磁盘或文件。这种病毒也是最难清除的。

6.3.1.3 计算机病毒的防护

网络反病毒技术包括预防病毒、检测病毒和消毒三种技术。

1. 预防病毒技术

预防病毒技术是指通过自身长驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统对系统进行破坏。这类技术有：加密可执行程序、引导区保护、系统监控与读写控制。

2. 检测病毒技术

检测病毒技术是指通过对计算机病毒的特征来进行判断的技术。如自身校验、关键字和文件长度的变化等。

3. 消毒技术

消毒技术是指通过对计算机病毒的分析而开发出的具有删除病毒程序并恢复原样的软件。

网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁的扫描和检测，在工作站上用防病毒芯片和对网络目录以及文件设置访问权限等。

6.3.1.4　ARP 概念及攻击类型和防护原理

1. ARP 的概念

ARP 的全称是 Address Resolution Protocol，中文名为地址解析协议，它工作在数据链路层，发的是广播(MAC 地址为 FF-FF-FF-FF-FF-FF)。在数据传输过程中，数据要封装成以太网帧(其帧格式如图 6-39 所示)，当需要目的 MAC 地址时，就通过 ARP 广播来请求。

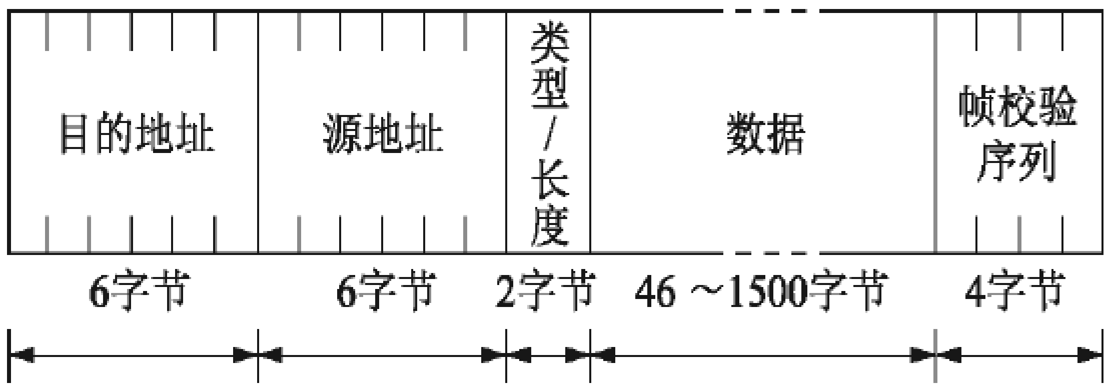


图 6-39　标准以太网帧格式

2. ARP 的工作原理

在 OSI 七层模型中，曾讲到数据在传输的过程中要进行不断地封装与解封装。当封装到第二层数据链路层时，需要知道源 MAC 地址与目的 MAC 地址，源 MAC 地址是自己网卡的，那么目的 MAC 地址如何得到呢？这时就需要主机发一个 ARP 广播来请求目的 IP 所对应的 MAC 地址，当目的主机与本机在同一个网段时，就能收到广播，给出单播回应；当目的主机在另外一个网段时，三层设备不转发广播，目的主机收不到请求，就不能回应，那怎么办呢？这时，主机的网关就会将自己的 MAC 地址回应给主机，这叫代理 ARP。

例如：

A 的地址为 IP：192.168.10.11/24；MAC：AA-AA-AA-AA-AA-AA。

B 的地址为 IP：192.168.10.12 /24；MAC：BB-BB-BB-BB-BB-BB。

A 与 B 的网关 IP：192.168.10.1/24；MAC：CC-CC-CC-CC-CC-CC。

A 向 B 发包时

IP 包头中：源 IP 为 192.168.10.11，目的 IP 为 192.168.10.12。

以太网帧头中：源 MAC 为 AA-AA-AA-AA-AA-AA，目的 MAC 为 BB-BB-BB-BB-BB-BB。

A 向 192.168.20.2/24 发包时

IP 包头中：源 IP 为 192.168.10.11，目的 IP 为 192.168.20.2。

以太网帧头中：源 MAC 为 AA-AA-AA-AA-AA-AA，目的 MAC 为 CC-CC-CC-CC-CC-CC。

3. 常见 ARP 攻击类型

1) ARP 扫描(ARP 请求风暴)

(1) 通信模式：请求→请求→请求→请求→请求→请求→应答→请求→请求→请求……

(2) 描述：网络中出现大量的 ARP 请求广播包，几乎都是对网段内的所有主机进行扫描。大量的 ARP 请求广播可能会占用网络带宽资源；ARP 扫描一般为 ARP 攻击的前奏。

(3) 出现原因：病毒程序、侦听程序、扫描程序。

2) ARP 欺骗

ARP 协议并不只在发送了 ARP 请求后才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。所以在网络中，如果有人发送一个自己伪造的 ARP 应答，网络可能就会出现问题。

假设一个网络环境中，网内有三台主机，分别为主机 A、B、C。

主机详细信息描述如下。

A 的地址为：IP 地址是 192.168.10.1，MAC 地址是 AA-AA-AA-AA-AA-AA。

B 的地址为：IP 地址是 192.168.10.2，MAC 地址是 BB-BB-BB-BB-BB-BB。

C 的地址为：IP 地址是 192.168.10.3，MAC 地址是 CC-CC-CC-CC-CC-CC。

正常情况下 A 和 C 之间进行通信，但是此时 B 向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据为“发送方 IP 地址是 192.168.10.3(C 的 IP 地址)，MAC 地址是 BB-BB-BB-BB-BB-BB(C 的 MAC 地址本来应该是 CC-CC-CC-CC-CC-CC，这里被伪造了)”。当 A 接收到 B 伪造的 ARP 应答，就会更新本地的 ARP 缓存(A 被欺骗了)，这时 B 就伪装成 C 了。同时，B 同样向 C 发送一个 ARP 应答，应答包中发送方 IP 地址是 192.168.10.1(A 的 IP 地址)，MAC 地址是 BB-BB-BB-BB-BB-BB(A 的 MAC 地址本来应该是 AA-AA-AA-AA-AA-AA)，当 C 收到 B 伪造的 ARP 应答，也会更新本地 ARP 缓存(C 也被欺骗了)，这时 B 就伪装成了 A。这样主机 A 和 C 都被主机 B 欺骗，A 和 C 之间通信的数据都经过了 B。主机 B 完全可以知道它们之间说的什么。这就是典型的 ARP 欺骗过程。

ARP 欺骗存在两种情况：一种是欺骗主机作为“中间人”，被欺骗主机的数据都经过它中转一次，这样欺骗主机可以窃取到被它欺骗的主机之间的通信数据；另一种是让被欺骗主机直接断网。

(1) 第一种：窃取数据(嗅探)。

① 通信模式：应答→应答→应答→应答→应答→请求→应答→应答→请求→应答……

② 描述：这种情况就属于上面所说的典型的 ARP 欺骗，欺骗主机向被欺骗主机发送大量伪造的 ARP 应答包进行欺骗，当通信双方被欺骗成功后，自己成为一个“中间人”。此时被欺骗的主机双方还能正常通信，只不过在通信过程中被欺骗者“窃听”了。

③ 出现原因：木马病毒、嗅探和人为欺骗。

(2) 第二种：导致断网。

① 通信模式：应答→应答→应答→应答→应答→应答→请求……

② 描述：这类情况就是在 ARP 欺骗过程中，欺骗者只欺骗了其中一方，如 B 欺骗了 A，但是同时 B 没有对 C 进行欺骗，这样 A 实质上是在和 B 通信，所以 A 就不能和 C 通信了，另外一种情况就是欺骗者还可能伪造一个不存在的地址进行欺骗。

③ 出现原因：木马病毒、人为破坏和一些网管软件的控制功能。

4. 常用的防护方法

目前对于 ARP 攻击防护主要有两种方法，一种是绑定 IP 和 MAC，另一种是使用 ARP 防护软件。另外，也出现了具有 ARP 防护功能的路由器。我们来了解一下前两种方法。

1) 静态绑定

最常用的方法就是进行 IP 和 MAC 静态绑定，在网内把主机和网关都进行 IP 和 MAC 绑定。

欺骗是通过 ARP 动态实时的规则欺骗内网机器，所以把 ARP 全部设置为静态，这样可以解决对内网 PC 的欺骗，同时在网关也要进行 IP 和 MAC 的静态绑定，这样双向绑定才比较保险。

静态绑定方法如下。

对每台主机进行 IP 和 MAC 地址静态绑定。

通过命令 arp -s 可以实现 IP 和 MAC 地址的静态绑定。

例如，使用 arp -s 命令，实现 IP 地址 192.168.10.1 和物理地址 AA-AA-AA-AA-AA-AA 之间的静态绑定。

```
"arp -s 192.168.10.1 AA-AA-AA-AA-AA-AA"
```

如果设置成功，在 PC 上面执行 arp -a 时可以看到以下相关的提示。

```
Internet Address Physical Address Type
192.168.10.1 AA-AA-AA-AA-AA-AA static(静态)
```

注意：一般不绑定，在动态的情况下提示如下。

```
Internet Address Physical Address Type
192.168.10.1 AA-AA-AA-AA-AA-AA dynamic(动态)
```

说明：如果网络中有很多主机，如 500 台、1000 台等，如果对每一台都去做静态绑定，工作量是非常大的。这种静态绑定，在电脑每次重启后，都必须重新再绑定，虽然也可以做一个批处理文件，但还是比较麻烦。

2) 使用 ARP 防护软件

目前关于 ARP 类的防护软件出得比较多，比较常用的主要有 ARP 工具和 Antiarp 等。它们除了本身可以检测出 ARP 攻击外，防护的工作原理是以一定频率向网络广播正确的 ARP 信息。

6.3.2 典型例题分析

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】 2007 年春，ARP 木马大范围流行。木马发作时，计算机网络连接正常却无

法打开网页。由于 ARP 木马发出大量欺骗数据包，导致网络用户上网不稳定，甚至网络短时瘫痪。

【问题 1】(2 分)

ARP 木马利用 (1) 协议设计之初没有任何验证功能这一漏洞而实施破坏。

【问题 2】(3 分)

在以太网中，源主机以 (2) 方式向网络发送含有目的主机 IP 地址的 ARP 请求包；目的主机或另一个代表该主机的系统，以 (3) 方式返回一个含有目的主机 IP 地址及其 MAC 地址对的应答包。源主机将这个地址对缓存起来，以节约不必要的 ARP 通信开销。ARP 协议 (4) 必须在接收到 ARP 请求后才可以发送应答包。

(2)备选答案：

A. 单播　　B. 多播　　C. 广播　　D. 任意播

(3)备选答案：

A. 单播　　B. 多播　　C. 广播　　D. 任意播

(4)备选答案：

A. 规定　　B. 没有规定

【问题 3】(6 分)

ARP 木马利用感染主机向网络发送大量虚假 ARP 报文，主机 (5) 导致网络访问不稳定。例如，向被攻击主机发送的虚假 ARP 报文中，目的 IP 地址为 (6) ，目的 MAC 地址为 (7) ，这样会将同网段内其他主机发往网关的数据引向发送虚假 ARP 报文的机器，并抓取数据包截取用户口令信息。

(5)备选答案：

A. 只有感染 ARP 木马时才会

B. 没有感染 ARP 木马时也有可能

C. 感染 ARP 木马时一定会

D. 感染 ARP 木马时一定不会

(6)备选答案：

A. 网关 IP 地址　　B. 感染木马的主机 IP 地址

C. 网络广播 IP 地址　　D. 被攻击主机 IP 地址

(7)备选答案：

A. 网关 MAC 地址　　B. 被攻击主机 MAC 地址

C. 网络广播 MAC 地址　　D. 感染木马的主机 MAC 地址

【问题 4】(4 分)

网络正常时，运行如下命令，可以查看主机 ARP 缓存中的 IP 地址及其对应的 MAC 地址。

```
C:\>arp  (8)
```

(8)备选答案：

A. -s　　B. -d　　C. -all　　D. -a

假设在某主机运行上述命令后，显示如图 6-40 所示信息。

```
Interface: 172.30.1.13 --- 0x30002
  Internet Address      Physical Address      Type
  172.30.0.1            00-10-db-92-aa-30     dynamic
```

图 6-40　命令结果信息

00-10-db-92-aa-30 是正确的 MAC 地址。在网络感染 ARP 木马时，运行上述命令可能显示如图 6-41 所示信息。

```
Interface: 172.30.1.13 --- 0x30002
  Internet Address      Physical Address      Type
  172.30.0.1            00-10-db-92-00-31     dynamic
```

图 6-41　命令显示信息

当发现主机 ARP 缓存中的 MAC 地址不正确时，可以执行如下命令清除 ARP 缓存。

C:\>ARP __(9)__

(9)备选答案：

A. -s　　B. -d　　C. -all　　D. -a

之后，重新绑定 MAC 地址，命令如下。

C:\>ARP -s __(10)__ __(11)__

(10)备选答案：

A. 172.30.0.1　　B. 172.30.1.13

C. 00-10-db-92-aa-30　　D. 00-10-db-92-00-31

(11)备选答案：

A. 172.30.0.1　　B. 172.30.1.13

C. 00-10-db-92-aa-30　　D. 00-10-db-92-00-31

答案：

【问题 1】

(1) ARP 或地址解析协议

【问题 2】

(2) C　(3) A　(4) B

【问题 3】

(5) B　(6) A　(7) D

【问题 4】

(8) D　(9) B　(10) A　(11) C

解析：

本题考查的是有关 ARP 协议和 ARP 攻击的基础知识，以及对 ARP 攻击进行简单处理所需要掌握的基础知识。

【问题 1】 本问题考查 ARP 攻击的基本原理。ARP 木马利用 ARP 协议在设计之初没有任何验证功能这一漏洞而实施破坏。

【问题 2】 源主机以广播方式向网络发送含有目的主机 IP 地址的 ARP 请求包；目的

主机或另一个代表该主机的系统，以单播方式返回一个含有目的主机 IP 地址及其 MAC 地址对的应答包。源主机将这个地址对进行缓存，以节约不必要的 ARP 通信开销。ARP 协议没有规定必须在接收到 ARP 请求后才可以发送应答包，这也是 ARP 协议的重要漏洞之一。

【问题 3】 感染 ARP 木马的主机会向网络发送大量虚假 ARP 报文，影响其他主机正常上网。因此，如果某个主机没有感染 ARP 木马，有可能受其他感染木马的主机发送的虚假报文的影响而导致网络访问不稳定。本问题中的例子是一个典型的 ARP 木马攻击方式，感染 ARP 木马的主机向被攻击主机发送的虚假 ARP 报文中，目的 IP 地址为网关 IP 地址，目的 MAC 地址为感染木马的主机 MAC 地址，会将同网段内其他主机发往网关的数据引向发送虚假 ARP 报文的机器。

【问题 4】 本问题考查使用命令行工具 ARP 配置 Windows，解决 ARP 攻击的技能。

在 TCP/IP 中，ARP 是一种利用本地网络上的广播通信解析到达其物理硬件的以逻辑方式分配的 IP 地址或媒体访问控制层地址的协议。

ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 arp 命令将显示帮助信息。

语法与相关参数如下。

- -a [InetAddr] [-N IfaceAddr]: 显示指定 IP 地址的 ARP 缓存项，要使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表指定的 IP 地址。要显示指定接口的 ARP 缓存表，使用-N Iface-Addr 参数，此处的 IfaceAddr 代表分配给指定接口的 IP 地址。-N 参数分大小写。
- -g [InetAddr] [-N IfaceAddr]: 与-a 相同。
- -d InetAddr [IfaceAddr]: 删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该接口的 IP 地址。要删除所有项，请使用星号(*)通配符代替 InetAddr。
- -s InetAddr EtherAddr [IfaceAddr]: 向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该接口的 IP 地址。

InetAddr 和 IfaceAddr 的 IP 地址用带圆点的十进制记数法表示。

物理地址 EtherAddr 由六个字节组成，这些字节用十六进制记数法表示并且用连字符隔开(如 00-AA-00-4F-2A-9C)。

由本题可知网关的 IP 为 172.30.0.1，相对应的正确的物理地址为 00-10-db-92-aa-30。要添加将 IP 地址 172.30.0.1 解析成物理地址 00-10-db-92-aa-30 的静态 ARP 缓存项，可输入:

```
arp -s 172.30.0.1 00-10-db-92-aa-30
```

6.3.3 同步练习

计算机病毒的常见类型有哪些？其工作原理是什么？举例说明。

6.3.4 同步练习参考答案

答案：见 6.3.1.2 节。

6.4 本章小结

本章知识点在 2014 年的新大纲中变化较大，增加了网络安全方面的内容，包括访问控制与防火墙、数字证书、VPN 配置、PGP 和病毒防护。

本章主要要求考生掌握防火墙的知识和访问控制策略，包括 ACL 命令、过滤规则和 Cisco PIX 防火墙的配置；考生还要掌握 VPN 的实现与配置，还有一些病毒防护的知识。

本章内容为下午科目的重点内容，为每次考试的必考内容。其中防火墙的配置和 VPN 是考试重点，尤其是 ACL 和 VPN 的实现是每年必考内容。本章的每小节针对考试大纲，组织了近 5 年来的真题和小部分模拟题，这些题目将有助于考生理解和掌握大纲中的知识点。

参 考 文 献

[1] 全国计算机技术与软件专业技术资格(水平)考试办公室. 网络工程师考试大纲与培训指南(2009版)[M]. 北京：清华大学出版社，2009.

[2] 全国计算机技术与软件专业技术资格(水平)考试办公室. 网络工程师历年试题分析与解答[M]. 北京：清华大学出版社，2008.

[3] 雷震甲. 网络工程师教程(第三版)(修订版)[M]. 北京：清华大学出版社，2012.

[4] 李磊. 网络工程师考试辅导(2009 版)[M]. 北京：清华大学出版社，2009.

[5] 施游，桂阳. 网络工程师考试考点分析与真题详解(最新版)[M]. 北京：电子工业出版社，2009.

[6] 黄传河. 网络规划设计师教程[M]. 北京：清华大学出版社，2009.

[7] 施游，张友生. 网络规划设计师考试全程指导[M]. 北京：清华大学出版社，2009.

[8] (美)希尔. Cisco 完全手册[M]. 北京：电子工业出版社，2008.

[9] (美)Richard Deal. CiscoVPN 完全配置指南[M]. 北京：人民邮电出版社，2007.

[10] 鸟哥. 鸟哥的 Linux 私房菜基础学习篇(第二版)[M]. 北京：人民邮电出版社，2007.

[11] IT 同路人. Linux 标准学习教程[M]. 北京：人民邮电出版社，2008.

[12] William R. Stanek. Microsoft® Windows Server(TM) 2003 Administrator's Pocket Consultant, Second Edition[M]. Microsoft Press，2006.

[13] 赵江，董欣. Windows Server 2003 中文版从入门到精通[M]. 北京：电子工业出版社，2008.

[14] (美) Brian Morgan, Craig Dennis 著；张宜春等译. CCNP BCRAN 认证考试(642-821)指南[M]. 北京：人民邮电出版社，2004.

[15] (美)Diane Teare. CCDA 自学指南[M]. 北京：人民邮电出版社，2004.

[16] 蔡建新. Cisco CCNP/CCIP 网络工程师[M]. 北京：清华大学出版社，2004.

[17] 柴晓路等. Web Services 技术、架构和应用[M]. 北京：电子工业出版社，2003.

[18] (美) Al Williams 著；何雄等译. Java 2 网络协议内幕[M]. 北京：中国水利水电出版社，2002.

[19] (美) Ed Roman 著；刘晓华译. 精通 EJB(第二版)[M]. 北京：电子工业出版社，2002.